BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19) Japanese Patent Office (JP)
(12) Publication of Patent Applications (A)
(11) Patent application publication number
Kokai (unexamined patent publication) NO. 2000-20377
(P2000-20377A)
(43) Publication date: January 21, 2000
Domestic classification symbol
Theme code (for reference)
Request for examination
Not requested
Number of claims: 18
(14 pages in total)
(21) Application No.: Patent application No.11-324859
(22) Filing date: June 30, 1998
(71) Applicant: 000006769
LION CORPORATION
1-3-7, Honjo, Sumida-ku, Tokyo
(71) Applicant: 000131201
CSK Co., Ltd.
2-6-1, Nish-shinjuku, Shinjuku-ku, Tokyo
(72) Inventor: Toyoyuki Sato
c/o LION CORPORATION, 1-3-7, Honjo, Sumida-ku, Tokyo
(74) Representative: 100081961
Mitsuharu Kiuchi, patent attorney
Continued to the last page

(54) Title of the Invention
Database system, data management method and recording medium that records software for data management

(57) [Abstract]
[Purpose] To correlate an access right with an organizational attribute of a user and thereby change data management easily

[Means for accomplishing the purpose]
A document access designation unit 42 designates what mode (kind)

of access such as reference, making and approval should be made and to which document in a database 1. A document making and reference right check unit 43 judges whether a user has an access right to the designated document and the kind of access based on the section he belongs to and his post. A page making and reference right check unit 45 checks whether the user has an access right to reference and making for the part of document designated by a document contents indication unit 44 and the kind of access. A page indication and writing unit 46 indicates the page of the designated document.

1 Database
2 Database management system
3 Display input interface unit
4 Document management control unit
41 User check unit
42 Document access designation unit
43 Document making and reference right check unit
44 Document contents indication unit
45 Page making and reference right check unit
46 Page indication and writing unit

[Scope of claim for patent]

[Claim 1] A database system that manages data, comprising:

a device that designates which data a user should access;

a judgement device that judges whether the user has an access right to the designated data based on the organizational attribute that is given to each user in advance; and

an access device that makes the user who is judged to have an access right access the designated data.

[Claim 2] The database system according to claim 1, further comprising:

when a user is judged to have an access right to the designated data,

a device that indicates what part of data the designated data has;

a device that designates what part of data the user should access; and

a second judgement device that judges whether the user has an access right to the designated part of data based on the organizational attribute that is given to each user in advance, wherein

the access device makes the user who is judged to have an access right to the designated part of data access said part of data.

[Claim 3] The database system according to claim 1 or 2, wherein

each of data is classified into a plurality of groups in advance; and

the judgement device judges whether a user has an access right to the designated data based on the correlation of the classification of the designated data with the organizational attribute that is given to each user in advance.

[Claim 4] The database system that manages data, comprising:

an attribute table that correlates each user with the section that he belongs to and his post;

a classification table that classifies data into a group of data including one of data, or two or more of data and a large group of data including one group of data, or two or more groups of data;

a table that correlates one version, or two or more versions of each data with the pages included in the data and at least one of either one version, or two or more versions of each page; and

an access right table that stores whether the user has an access right to the data, for at lest one each of the group of data, a large group of data, data, versions of data, pages and versions of pages, based on at least one of either the section that the user belongs to or his post.

[Claim 5] The database system that manages data,

comprising:

an access right table that stores what kind of organizational attribute a user has and what kind of access right he has for data or a part of data;

a device that checks whether the user has the right to use the database system;

a device that designates the data that the user will access;

a device that judges whether the user has an access right to the designated data based on his organizational attribute and the access right table;

a device that indicates what parts of data the data has when the user has an access right to the designated data;

a device that designates the part of data that the user will access and the kind of access;

a device that judges whether the user has an access right to the designated part of data and the kind of access based on the access right table; and

an access device that makes the user execute an access right when the user has an access right to the designated part of data and the kind of access.

[Claim 6] The database system that manages data,
comprising:

An attribute table that stores the organizational attribute of each user;

An access right table that stores whether the user has an access right to each data based on the organizational attribute; and

a judgement device that judges whether each user is allowed to access the designated data based on the attribute table and the access right table.

[Claim 7] The database system according to claim 6, further comprising:

a classification table that classifies individual data into a plurality of groups including one or more hierarchies,

wherein

the access right table stores whether the user has an access right to data based on each individual classification.

[Claim 8] The database system according to claim 6 or claim 7, wherein

the attribute table includes at least one of either the section that a user belongs to or his post; and

the access right table stores whether the user has an access right to data based on at least one of either the section that the user belongs to or his post.

[Claim 9] The database system according to one of claims 6 to 8, wherein

the access right table stores whether a user has an access right according to the kind of access.

[Claim 10] The database system according to one of claims 6 to 9, wherein

the access right table stores whether a user has an access right based on at least one of either the version of data, pages included in the data or versions of pages as a unit; and

the judgement device is so constituted as to judge whether the user is allowed to access the version, pages or versions of pages designated to data.

[Claim 11] The database system according to one of claims 6 to 10, further comprising:

a table that limits the access to at least one of the data, version of data, pages or versions of pages only to a part of the users of the section.

[Claim 12] The database system according to claim 10 or claim 11, further comprising:

a table that stores the contents of data for each page.

[Claim 13] The data management method that manages data, including:

a step of designating which data a user should access;

a step of judging whether the user has an access right to the designated data based on the organizational attribute that is give to each user in advance; and

a step of making the user who is judged to have an access right access the designated data.

[Claim 14] The data management method according to claim 13, including:

when a user is judged to have an access right to the designated data,

a step of indicating what part of data the designated data has;

a step of designating what part of data the user should access; and

a step of judging whether the user has an access right to the designated part of data based on the organizational attribute that is given to each user in advance,

wherein

the access step makes the user who is judged to have an access right to the designated part of data access said part of data.

[Claim 15] The data management method according to claim 13 or claim 14, wherein

each of data is classified into a plurality of groups in advance; and

the judgement step judges whether a user has an access right to the designated data based on the correlation of the classification of the designated data with the organizational attribute that is given to each user in advance.

[Claim 16] The data management method for managing data, which uses:

an attribute table that correlates each user with the section

that he belongs to and his post;

a classification table that classifies data into a group of data including one of data, or two or more of data and a large group of data including one group of data ,or two or more groups of data;

a table that correlates one version, or two or more versions of each of data with the pages included in the data and at least one of either one version, or two or more versions of each page; and

an access right table that stores whether the user has an access right to the data, for at lest one each of the group of data, a large group of data, data, versions of data, pages and versions of pages, based on at least one of either the section that the user belongs to or his post.

[Claim 17] A recording medium that records software for data management that manages data using a computer, wherein

the software makes the computer receive the designation as to which data a user accesses and judge whether the user has an access right to the designated data based on the organizational attribute that is given to each user in advance; and

the software makes the user who is judged to have an access right access the designated data.

[Claim 18] The recording medium that records software for data management according to claim 17, wherein

the software makes the computer indicate what part of data the designated data has when the user is judged to have an access right to the designated data;

the software makes the computer receive the designation as to which part of data the user should access;

the software makes the computer judge whether the user has an access right to the designated part of data based on the organizational attribute that is given to each user in advance; and

the software makes the user who is judged to have an access

right to the designated part of data access said part of data.

[Detailed description of the invention]
[0001]
[Field of the Invention]
The present invention relates to the improvement of the technology pertaining to a database that stores and manages documents and the like, and more specifically to the technology that correlates an access right with the organizational attribute of a user and thereby changes data management easily.
[0002]
[Prior art] In the database that a plurality of users use, management of an access right is important to prevent an unlawful reference and alteration of documents, files and data (hereinafter referred to as "data"). The access right is the right that represents which user can access what data and how, and generally, it is set according to the kind of access such as making, reference, edition and deletion.
[0003]
The following are the technologies pertaining to the management of the access right.
(1) The technology is known in which a password such as a key word and an access code is set using data as a unit and which allows the user who knows the password to access the file.
[0004]
(2) The technology is also known in which an access right is set as a unit using a group of data consisting of a directory, etc. as a unit, and which limits for which group of data the access is permitted based on the user ID and password that the user inputs.
[0005]
(3) Furthermore, the technology is known which sets the possibility, yes or no, with regard to a plurality of authority, for example, when a user accesses a group of data, which item of the data the user can operate, and what kind operation can be permitted, and which can assign the kind of the authority

related to each data group to each individual user, as disclosed in Kokai (unexamined patent publication) No. 9-6681.

[0006]

(4) Disclosed in Patent No. 2700517 (Kokai (unexpected patent publication) No. 6-266591) is an example in which for the data management using a relational database, each version of data and each version in page units of data are correlated with each other and are stored at the same time. In this example, the kind of secrecy can be also set to each version and page, and the access right can be managed based on the attribute of each user.

[0007]

[Problems to be solved by the invention] In the prior art described above, however, since an access right was managed for each individual user independently of his organizational section or post, there was a problem in that to make a change related to an access right was a bothersome job when the kind of data increased or personnel reshuffling occurred.

[0008]

In the case of (1) above, since a password was set to data as a target, it was not possible to use the data unless each user who uses the data to do a common service was informed of the password. Thus, there was a problem in that it took some time and labor to let the users in a necessary range know the password, and as the kind of password increases, the users had a heavy burden of managing the increased passwords. Furthermore, when a user who knew a password lost his access right to data owing to his reshuffling, etc., a complicated procedure for changing the password, etc. was required.

[0009]

In the case of (2) above, the ID and password that correspond to a group of data must have been made known only to each user who can access the group of data. When the user lost his access right, for example, because he changed his job due to personnel reshuffling, it was difficult to carry out the management of preventing a user having an original access right from making unauthorized access.

[0010]
In the case of (3) above, since an access right was set in the relationship between each user and the operable items or contents, the setting of the access right was complicated. In particular, when he changed the section he belonged to due to personnel reshuffling, etc. and his access right changed accordingly, the access right must have been set again in the relationship between each user and the operable items or contents, thereby causing the user to bear a burden of time and labor.
[0011]
Particularly, with regard to the access right within an organization like a company, both the viewpoint of what level-post of user can access data, and the viewpoint of which section of user is reasonably allowed to access data are required. In prior art, however, the viewpoint that should be a plurality of viewpoints was centralized in a table that indicates access rights. As a consequence, when personnel reshuffling took place, reorganization of departments took place, or data increased, such a centralized table must have been corrected in the relationship of each individual person without any contradiction, and it took a lot of time and labor to correct the centralized table exactly.
[0012]
The present invention has been developed to solve the problems existing in the prior art as mentioned above. One purpose of the present invention is to correlate an access right with the organizational attribute of a user and thereby change data management easily, and another purpose of the present invention is to set access rights to a plurality of documents collectively and efficiently. Also, another purpose of the present invention is to cause an access right to be set for each part of a document and thereby manage security meticulously.
[0013]
[Means for solving the problems] In order to accomplish the above-mentioned purposes, the invention according to claim 1 comprises, in a databases system that manages data,

a device that designates which data a user should access;

a judgement device that judges whether the user has an access right to the designated data based on the organizational attribute that is given to each user in advance; and

an access device that makes the user who is judged to have an access right access the designated data.

The invention according to claim 6 indicates a data structure of a table in connection with the invention according to claim 1, and comprises, in a database system that manages data,

an attribute table that stores the organizational attribute of each user;

an access right table that stores whether the user has an access right to each data based on the organizational attribute; and

a judgement device that judges whether each user is allowed to access the designated data based on the attribute table and the access right table.

The invention according to claim 13 is the one that views the invention according to claim 1 from the viewpoint of a method, and comprises, in a data management method that manages data,

a step of designating which data the user should access;

a step of judging whether the user has an access right to the designated data base on the organizational attribute that is give to each user in advance; and

a step of making the user who is judged to have an access right access the designated data.

The invention according to claim 17 is the one that views the invention according to claims 1 and 13 from the viewpoint of a recording medium that records software of a computer, and in a recording medium that records software for data management that manages data using a computer,

the software makes the computer receive the designation as to which data the user accesses and judge whether the user has an access right to the designated data based on the organizational attribute that is given to each user in advance; and

the software makes the user who is judged to have an access

right access the designated data.

In the invention according to claims 1, 6, 13 and 17, whether a user is allowed to access each of data is judged based on the organizational attribute such as the user's section and post. Therefore, when his section and post change due to personnel reshuffling, if he changes his organizational attribute, the contents of the access right automatically change together. Consequently, it becomes unnecessary to take the trouble of inputting his password for each of data which he accesses, and of changing his password or setting his access right for each of data again when personnel reshuffling takes place.

[0014]

The invention according to claim 2 comprises, in the database system according to claim 1,

when the user is judged to have an access right to the designated data,

a device that indicates what part of data the designated data has;

a device that designates what part of data the user should access; and

a second judgement device that judges whether the user has an access right to the designated part of data based on the organizational attribute that is given to each user in advance, wherein

the access device makes the user who is judged to have an access right to the designated part of data access said part of data.

The invention according to claim 5 comprises, in a database system that manages data,

an access right table that stores what kind of organizational attribute a user has and what kind of access right he has for data or a part of data;

a device that checks whether the user has the right to use a database system;

a device that designates the data that the user he will access;

a device that judges whether the user has the access right

to the designated data based on the user's organizational attribute and the access right table;

a device that indicates what part of data the data has when the user has an access right to the designated data;

a device that designates the part of data that the user will access and the kind of access;

a device that judges whether the user has an access right to the designated part of data and the kind of access based on the access right table; and

an access device that makes the user execute an access right when the user has an access right to the designated part of data and the kind of access.

The invention according to claim 14 is the one that views the invention according to claim 2 from the viewpoint of a method, and includes, in the data management method according to 13,

when the user is judged to have an access right to the designated data,

a step of indicating what part of data the designated data has;

a step of designating what part of data the user should access; and

a step of judging whether the user has an access right to the designated part of data based on the organizational attribute that is given to each user in advance,

wherein

the access step makes the user who is judged to have an access right to the designated part of data access said part of data.

The invention according to claim 18 is the one that views the invention according to claims 2 and 14 from the viewpoint of a recording medium that records software for a computer, wherein, in the database system according to claim 17,

the software makes the computer indicate what part of data the designated data has when the user is judged to have an access right to the designated data;

the software makes the computer receive the designation as to which part of data the user should access;

the software makes the computer judge whether the user has an access right to the designated part of data based on the organizational attribute that is given to each user in advance; and

the software makes the user who is judged to have an access right to the designated part of data access said part of data.

In the invention according to claims 2, 5, 14 and 18, what part of data such as version and page the data has is indicated only when it is confirmed whether a user has an access right to the data in addition to when it is checked whether the user has the right to use the database system when logging in. Moreover, an access right is confirmed with regard to the part of data that the user will access and the kind of access. Thus, security of the system is further improved by disclosing information to users step by step.

[0015]

The invention according to claim 3 comprises, in the database system according to claims 1 and 2,

each of data is classified into a plurality of groups in advance; and

the judgement device judges whether the user has an access right to the designated data based on the correlation of the classification of the designated data with the organizational attribute that is given to each user in advance.

The invention according to claim 7 indicates a data structure of a table in connection with the invention according to claim 3, and comprises, in the database system according to claim 6,

a classification table that classifies individual data into a plurality of groups including one or more hierarchies, wherein

the access right table stores whether the user has an access right to data based on each individual classification.

The invention according to claim 15 is the one that views the invention according to claim 3 from the viewpoint of a method, wherein, in the data management method according to claims 13 and 14,

each of data is classified into a plurality of groups in advance; and

the judgement step judges whether the user has an access right to the designated data based on the correlation of the classification of the designated data with the organizational attribute that is given to each user in advance.

In the invention according to claims 3, 7, and 15, it is possible to set access rights with regard to a plurality of data having a common character collectively and efficiently using the kind of data and a superordinate concept such as a higher-ranked large classification.

[0016]

The invention according to claim 4 comprises, in the database system that manages data,

an attribute table that correlates each user with the section that he belongs to and his post;

a classification table that classifies data into a group of data including one of data, or two or more of data and a large group of data including one group of data or two or more groups of data;

a table that correlates one version, or two or more versions of each of data with the pages included in the data and at least one of either one version, or two or more versions of each page; and

an access right table that stores whether the user has an access right to the data, for at lest one each of the group of data, a large group of data, data, versions of data, pages and versions of pages, based on at least one of either the section that the user belongs to or his post. The invention according to claim 16 is the one that views the invention according to claim 4 from the viewpoint of a method, and uses, in the data management method that manages data,

an attribute table that correlates each user with the section that he belongs to and his post in advance;

a classification table that classifies data into a group of data including one of data, or two or more of data and a large

group of data including one group of data, or two or more groups of data;

a table that correlates one version, or two or more versions of each data with the pages included in the data and at least one of either one version, or two or more versions of each page; and

an access right table that stores whether the user has an access right to the data, for at lest one each of the group of data, a large group of data, data, versions of data, pages and versions of pages, based on at least one of either the section that the user belongs to or his post. In the invention according to claims 4, and 16, it is possible to set access rights to data collectively using a superordinate concept such as a kind of data and a large classification, or using part of data such as every version or every page as a unit. It is also possible to set access rights using these as units based on the section he belongs to or his post. Consequently, sharing of information and security can be competent with each other by disclosing an appropriate kind of data or an appropriate part of data to an competent person holding a managerial post in a section concerned. As a processing procedure using these tables, such a procedure can be considered in which after a user confirms an access right using data as a unit, the user can see what version or page exists, and when he further selects the version or page he will access based on that, an concrete access right is confirmed for the selected version or page. Also, each table can be constituted as an each individual table or can be constituted, for example, as a plurality of tables according to each kind of correlative relationship.

[0017]

The invention according to claim 8 comprises, in the database system according to claims 6 and 7,

the attribute table includes at least one of either the section that the user belongs to or his post; and

the access right table stores whether the user has an access right to data based on at least one of either the section that

the user belongs to or his post.
In the invention according to claim 8, since it is judged whether the user has an access right to data based on the section he belongs to or his post, this invention according to claim 8 can be easily applied to many organizations that have a systematical hierarchical-post system for each section.
[0018]

The invention according to claim 9 comprises, in one of the database systems according to one of claims 6 through 8,

the access right table stores whether the user has an access right according to the kind of access.

In the invention according to claim 9, since an access right can be set according to the kind of access such as reference for only seeing data, making data and approval of data, security can be properly managed according to the flow of business and the scope of authorities.
[0019]

The invention according to 10 comprises, in the database systems according to one of claims 6 through claim 9,

the access right table stores whether the user has an access right based on at least one of either the version of data, pages included in the data or versions of pages as a unit; and

the judgement device is so constituted as to judge whether the user is allowed to access the version, pages or versions of pages designated to data.

In the invention according to claim 10, an access right to data such as a document can be set using a part of data such as each version and each page as a unit. Consequently, when a character differs depending on a part of even one kind of data, it is not necessary to decide whether the user is allowed to access the data as a whole. Thus, it is possible to properly set whether priority is placed on the use of information by allowing the user to access the data or whether priority is placed on security without allowing the user to access the data.
[0020]

The invention according to claim 11 comprises, in the database

system according to one of claims 6 to 10,

a table that limits the access to at lest one of the data, version of data, pages or versions of pages only to a part of the users of the section.

In the invention according to claim 11, with regard to the data that is the confidential matters that must be made secret to other sections in an organization and the data that cannot be disclosed to other sections because the data is being made yet, access can be limited to only the users of a part of the sections such as the section that makes the data, thus causing security to be further improved.

[0021]

The invention according to claim 12 comprises a table that stores the contents of data for each page in the database system according to claim 10 or claim 11. In the invention according to claim 12, the contents of each page can be stored in the form of an easy-to-use table on a relational database, thereby causing the storage to be implemented easily.

[0022]

[Mode for carrying out the invention] Described below is the mode for carrying out the present invention (hereinafter referred to as "embodiment") with reference to the accompanying drawings. It is considered to be general to realize the present invention by controlling a computer having peripheral devices by means of software. In this case, the software is made by a combination of commands in accordance with the description of this specification, and the technique that was explained in the prior art is also used for the part common to prior art. The software includes not only a program code but also data that is prepared in advance to execute the program code.

[0023]

The software realizes the operation and effect of the present invention by making use of physical resources such as a processing devices like a CPU, a coprocessor, and various kinds of chip sets; an input device like a keyboard and a mouse; a storage device like a memory and a hard disk; and an output device like

a display and a printer.

[0024]

The constitution of the software and hardware that realize the present invention can be changed to various kinds of constitutions. For example, there are a compiler, an interpreter, and an assembler in the type of software, and a network connection device and an attachable and detachable recording medium such as a floppy disk can be considered in order to exchange information with outside. Also, a recording medium such as the CD-ROM that records the software and program to realize the present invention is an embodiment of the present invention by itself. Furthermore, part of the functions of the present invention can be realized by a physical electronic circuit such as an LSI.

[0025]

Thus, various kinds of modes for carrying out the present invention using a computer can be considered. Described below are the present invention and the embodiment using a virtual circuit block that realizes each function included in the present invention and the embodiment. In regard to the drawings which will be used hereunder, like elements or similar kinds of elements are denoted by like reference numerals to omit explanations of the like elements each time.

[0026]

[1. Outline of embodiment] Fig. 1 is a conceptual diagram showing the outline of this embodiment. In this embodiment, data such as a document is stored in a database 1, attributes such as a section and a post of each user are stored in an attribute table H, and what attribute of user has an access right to reference and making with regard to each individual document stored in the database 1 is stored in an access right table T, as shown in Fig. 1. An output device 3a such as a CRT monitor and an input device 3b such as a keyboard and a mouse are provided as an interface that exchanges information such as directives and data with a user.

[0027]

When a user designates a document that he wants to access

from a designation device 142, a judgement device 143 refers to the attribute table H and the access right table T and judges whether the user has an access right to the designated document based on the organizational attribute of the user. When the user has the access right, an access device 146 executes the access to the designated document.

[0028]

[2. Constitution of embodiment]

[2-1. Overall constitution] Fig. 2 is a function block diagram showing a concrete constitution of this embodiment. This embodiment applies the present invention to a relational database, and comprises a database 1, a DBMS (database management system) 2, a display input interface unit 3 and a document management control unit 4, as shown in Fig. 2.

[0029]

The database 1 is a relational database, and can store a variety of data in the form of a table. Not only documents such as a character string text but also various kinds of files, e.g. files including decoration data peculiar to various kinds of application programs, graphics files such as a bit-map image, a worksheet for a table calculation program, and drawing data files for drawing tools and graphics software can be stored in the database 1.

[0030]

It is presumed that the database 1 stores documents as data here in this embodiment and that it also stores a plurality of tables to manage documents and manage an access right to the documents, as concretely described later.

[0031]

The DBMS 2 performs various operations such as making, addition, retrieval, updating and deletion with regard to the data such as documents stored in the database 1. The display input interface unit 3 is the interface that receives the input of various directives and data from a user and provides the user with data taken out from the database 1 and information of messages such as operational prompt.

[0032]

The document management control unit 4 refers to each table in the database 1 according to the directives given from the user via the display input interface unit 3 and makes the user having an access right access a document in the database 1. This document management control unit 4 comprises a user check unit 41, a document access designation unit 42, a document making and reference right check unit 43, a document contents indication unit 44, a page making and reference right check unit 45, and a page indication and writing unit 46.

[0033]

The user check unit 41 checks whether the user who is going to access the database 1 is a regular registered user based on his personal ID and password inputted from the display input interface unit 3, and captures his organizational attributes such as the section he belongs to and his post from a table in the database 1 in order to check his access right.

[0034]

The document access designation unit 42 designates what kind of document in the database 1 the user should access and what mode (kind) of access, reference, making or approval, he should make, and the document access designation unit 42 acquires the ID number of the document that uniquely determines which document the designated document is from a table in the database 1.

[0035]

The document making and reference right check unit 43 checks whether a user has a right to implement reference, making or approval for a designated document, i.e. an access right. If it is found that the user does not have this access right, the process cannot proceed to the next step like the step of document contents indication.

[0036]

The document contents indication unit 44 indicates the constitution (hereinafter referred to as "contents") of what version or what logical page (hereinafter referred to as "logical page" or "page") the designated document has in the form of a

table. The user sees the contents and designates which part, namely which version or which page of the document he wants to access, to the document contents indication unit 44, and also designates a mode such as a reference mode and a making mode as the kind of access.

[0037]

The page making and reference right check unit 45 checks whether the user has an access right to implement reference, making, etc. for the part designated by the document contents indication unit 44 and the kind of access, and if it is found that the user does not have this access right, the process does not proceed to the next step. The document making and reference right check unit 43 and the page making and reference right check unit 45 judge whether the access to the designated data is permitted to each individual user, and correspond to the second judgement device described in the scope of claim for patent.

[0038]

The page indication and writing unit 46 indicates the page of a designated document. In this page indication and writing unit 46, when a document is opened in a making mode, it is possible to write or rewrite the document in the displayed screen. However, when a document is opened in a reference mode, it is not possible to write or rewrite the document in the displayed screen. This page indication and writing unit 46 corresponds to the access device described in the scope of claim for patent.

[0039]

[2-2. Constitutions of the tables] The following tables required to manage documents and manage access rights are registered in the database 1. Table A shown in Fig 3 is a table that stores the document name, symbol and kind of document with regard to each individual document. Also, registered in the Table A are the document ID that is uniquely assigned to a document so that documents do not overlap with each other as well as what kind of document the document belongs to. Since documents are discriminated from each other by document ID's, the document name may not necessarily be unique (sole), but any document may

be freely named according to the application of the document.
[0040]

Table B shown in Fig. 4 indicates how many versions of documents and what version (hereinafter abbreviated to "document ver") of documents as a whole have been issued and stored for each document identified by document ID. For example, as a document whose document ID is "A001," there are two versions, version 1 and version 2, which are made at a different date.
[0041]

Table C shown in Fig. 5 stores what logic pages each version of the document identified by document ID in Table B shown in fig. 4 is composed of as well as what version (hereinafter referred to as "page version") each of the pages has.
[0042]

Table D shown in Fig. 6 correlates by which section each logic page and page version that constitute each document in Table C shown in Fig. 5 are made (namely, making section) with a secrecy level that is the information that limits an access right to part of sections.
[0043]

Table E shown in Fig. 7 classifies the kind of document correlated with each document in Table A shown in Fig. 3 into a large classification that is a superordinate concept. Thus, it is possible to easily set the access right for implementing making and reference using the superordinate concept of a large classification as a unit, as described in full detail later. Table A shown in Fig. 3 and Table E shown in Fig. 7 classify each individual document by means of two hierarchies, and correspond to the classification table mentioned above.
[0044]

Table F shown in Fig. 8 indicates a correlative relationship of what logic page should be included for each kind of document, and when a document is newly made or on some such occasion, any necessary page can be constituted by referring to this table.
[0045]

The contents of each individual logic page mentioned above

are stored in another table, and Table G shown in Fig. 9 indicates in which table the contents of each individual logic page are stored. Thus, by storing the contents of each individual logic page in a table, it is possible to constitute the table in the form of the same table in which the data itself and the data management table can be dealt with in a relational database, thereby causing the constitution to be implemented easily.
[0046]

Actual data that constitutes logic page PS01 (Fig. 9) as shown in Table G of Fig. 9 is divided into two according to the characteristics of data, and the divided data is stored in Tables TBL01 and TBL02 shown in Fig. 10 respectively. Likewise, Tables TBL31 and TBL32 shown in Fig. 11 stores actual data that constitutes another logic page PF01 (Fig. 9). Since the contents of these pages differ according to the applications of concrete documents and the application programs used, the contents of these pages do not need to be limited to a specific format, but can be set freely.
[0047]

Document Reference Right Table shown in Fig. 12 is a table in which what section of user or what post of user has an access right to access data in a reference mode is registered based on the large classification of documents or the kind of document. Likewise, Document Making Right Table shown in Fig. 13 is a table in which what section of user or what post of user has an access right to access data in a making mode is registered for each large classification and each kind of document.
[0048]

Page Reference Right Table shown in Fig. 14 is a table in which what section of user or what post of user has an access right to access data in a reference mode is registered for each logic page of a document. Likewise, Page Making Right Table shown in Fig. 14 is a table in which what section of user or what post of user has an access right to access data in a making mode is registered for each logic page of a document.
[0049]

Each of the tables shown in Figs. 12 to 14 stores whether a user has an access right to data based on the organizational attributes such as his section and post, and corresponds to the access right tables mentioned above. Theses access right tables store whether a user has an access right to data for each kind of access.

[0050]

Particularly, in the Page Reference Right Table and Page Making Right Table shown in Fig. 14, an access right is set for each page included in data, while in the access right table, an access right can be set for each version of documents and each version of pages.

[0051]

Table H shown in Fig. 15 stores the information related to each user who uses the system. Concretely speaking, Table H includes the section code of the section to which the user belongs and the post code that indicates his post in order to judge his access right in addition to his log-in name and password to confirm whether he is a regular registered user. The section and post are the organizational attributes of the user, and Table H corresponds to the attribute table mentioned above.

[0052]

[3. Operation of embodiment] The embodiment that is so constituted as described above operates as follows. Fig. 16 is a flowchart showing the processing procedure in this embodiment.

[3-1. User attestation and document designation] A user inputs his log-in name and password from the display input interface unit 3 (Step 1). When data related to the user is inputted, the user check unit 41 starts up in the document management control unit 4, and this user check unit 41 accesses Table H (Fig. 15) in the database 1 via DBMS 2 to check whether the user who corresponds to the inputted log-in name and password is registered.

[0053]

As a result, if it is found that the user who corresponds

to the inputted log-in name and password is registered (Step 2), the user check unit 41 reads the section code and post code of the logged-in user from Table H and stores them in the document management control unit 4, and then starts up the document access designation unit 42.

[0054]

When the user succeeds in log-in, the document access designation unit 42 indicates a list of documents of what documents are stored in the database 1 in the display input interface unit 3 based on the Table A (Fig. 3) in the database 1, and the user designates the document that he wants to access from the list of documents (Step 3). In this designation, the user identifies what document he wants to see by document ID, and identifies whether he only wants to refer to the document (reference mode) or he also wants to edit the document (making mode).

[0055]

It is completely free in what format documents are indicated, and no format related thereto is illustrated here. For example, a list of documents can be simply indicated in the order of document name or in the order of last updating date, or for example, documents can be indicated in a tree structure for each kind of documents or each directory of documents, or can be indicated according to the level of an access right.

[0056]

[3-2. Judgement of an access right in document units] Then, the document access designation unit 42 retrieves Table A (Fig. 3) in the database 1 based on the document ID of the designated document, and identifies the kind of document that corresponds to the designated document (Step 4). The document access designation unit 42 further retrieves Table E (Fig. 7) in the database 1 and acquires the large classification that corresponds to the kind of document (Step 5).

[0057]

Next, the document making and reference right check unit 43 in the document management control unit 4 collates the kind

of document and large classification acquired as described above and the user's section and post obtained from Table H with the document reference right table (Fig. 12) and document making right table (Fig. 13) in the database 1, and checks whether the user has an access right to refer or make the document that he designates (Step 6).

[0058]

For example, described below is how an access right is set in an example of the document reference right table shown in Fig. 12.

(1) With regard to the kind of document TS01, any user whose top three characters of the section he belongs to is BUA has a reference right.

(2) With regard to the kind of document TS02, any user whose post is A or B has a reference right regardless of what section he belongs to.

(3) With regard to the document that belongs to the large classification TS-B, e.g. the kind of document TS04 or TS05, any user of any section or post has a reference right regardless of the kind of document.

An asterisk "*" in the document reference right table (Fig. 12) or the document making right table (Fig. 13) indicates that there is no limit, i.e. a wild card. When a user is judged to have an access right in the check of Step 6, the document contents indication unit 44 is started up.

[0059]

[3-3. Judgement of an access right in page units] The document contents indication unit 44 retrieves Tables A, B, C and D (Figs. 3 to 6) in the database 1 based on the document ID of the document designated by the user, acquires information indicating which version, which page or which version of page the document is composed of, and indicates which version, which page or which version of page is in the document designated based on this information as well as the secrecy level and making section of each version, page or version of page (Step 7).

[0060]

The user designates which page or which version he wants to access, and in what mode he wants to access the page or version, in a reference or making mode, i.e. the kind of access (Step 7). Here, it is presumed that the user designates the object of access based on a logic page.

[0061]

Then, the page making and reference right check unit 45 checks whether the user has a making right and a reference right to the version, page and version of page designated as described above and the kind of access by retrieving the page reference right table and the page making right table (Fig. 14) (Step 8). In what format an access right is set in the page reference right table and the page making right table is the same as described above about the document reference right table (Fig. 12).

[0062]

Furthermore, the page making and reference right check unit 45 refers to the secrecy level stored in Table D (Fig. 6) in the database 1 with regard to the designated page version of the designated logic page (Step 9). This item of secrecy level temporarily limits the access right to a logic page of each individual document to part of sections and posts. For example, for the logic page in which secrecy level "J" is set in Fig. 6, no user other than the user of the section registered as the making section of the said logic page can refer to or make the logic page.

[0063]

When the section code in which the secrecy level other than "J" e.g. "BUA02" (Fig. 8) is set is set, no section other than the same section or making section as the set code can refer to or make the logic page. Shown here is an example in which a secrecy level is set for the page and page version of data. The secrecy level may be set using the whole document or the version of a document as a unit.

[0064]

[3-4. Access to pages] Only when a user is judged to have an access right through all the checks, the substance of the page

that the user designates is indicated by the page indication and writing unit 46, and it becomes possible to only refer to the page or to edit the contents according to the kind of access that the user designates (Step 10). On the other hand, if the user is judged not to have an access right through any of the checks in Steps 2, 6, 8 and 9, his access is rejected.

[0065]

Concretely speaking, the page indication and writing unit 46 retrieves the table name showing in which table the data corresponding to the designated logic page is stored from Table G (Fig. 9) in the database 1, and acquires and indicates the data corresponding to the designated document ID and logic page from the table having a table name thus retrieved e.g. Tables TBL01 and TBL02 (Fig. 10) and Tables TBL31 and TBL32 (Fig. 11).

[0066]

For example, as the result of referring to Table G, it becomes clear that the data indicating the contents of logic page PS01 are included in Tables TB01 and TB02, so the data of the page that the user designates can be acquired and indicated in the display input interface unit 3 by retrieving the corresponding document ID e.g. the data of A001 from Tables TBL01 and TBL02.

[0067]

When the user designates a "making" mode as the kind of access to the logic page, for example, a blinking cursor appears on the editable character string on the display screen, and when the user edits the contents using the cursor and operates termination, the contents so edited are rewritten in the corresponding table again, and the contents of the database 1 are updated.

[0068]

When a new version of a document, a new logic page and a new version of a logic page are made in this way, Table B and Table C are updated accordingly, and the parts that have been newly made are added to appropriate tables, thus being usable for subsequent access.

[0069]

[4. Effect of embodiment] As has been described, in this embodiment, whether a user is allowed to access each data is judged based on his organizational attributes stored in Table H, i.e. his section and post. When his section and post change owing to personnel reshuffling such as interdepartmental relocation, entering a company and leaving a company, maintenance of only the information that represents the attributes of each user suffices, and the contents of an access right automatically change accordingly.

[0070]

Thus, no time or labor is required to input a password for each data to be accessed, change a password when personnel reshuffling takes place, or re-set an access right for each data. In other words, the section and post of each user registered in Table H (Fig. 15) can be so constituted as to be changed directly from the Department of Personnel without using the information files as they are in the Department of Personnel or without doing any work in the Department of Information Processing.

[0071]

Consequently, when any change in a user's section or post takes place, no time or labor is required to newly re-set an access right from an access right point of view, and the access right can be easily managed without any contradiction in the relationship with other personnel information. After all, according to this embodiment, labor saving can be realized much more than prior art in which all information related to the access right of each individual user is changed or made.

[0072]

On the other hand, when a document making or reference right changes, for example, because the allotment of duties given to a section is changed, only the access tables such as a reference right table and a making right table can be changed, and information related to the attributes of each individual user does not need to be changed, thereby making the management of an access right easy.

[0073]

In this embodiment, access rights to a plurality of data having common characteristics can be effectively set in the lump using the kind of document shown in Table A (Fig. 3) and the superordinate concept of a large classification shown in Table E (Fig. 7), i.e. the binding unit that represents a plurality of documents.

[0074]

In particular, in this embodiment, whether a user has an access right is judged based on both his section and post, so it is easy to apply this embodiment to many organizations that are systematized in each section and department and have a hierarchical post system.

[0075]

Also, in this embodiment, since an access right can be set as shown in Figs. 12 to 14 according to the kind of access such as reference in which a document is only seen, making of a document and approval of the contents of a document, security can be accurately managed according to the flow of duties and the scope of authority.

[0076]

Also, in this embodiment, an access right to data such as a document can be set using the part such as each version or each page as a unit. Consequently, when one kind of data differs in character according to its parts, it is not necessary to forcibly decide whether access is permitted or not as the whole data. It is thus possible to set whether priority should be place on the usage of information by permitting access or whether priority should be placed on security without permitting access according to the characters of the parts.

[0077]

Also, in this embodiment, with regard to the data related to confidential matters that must be kept secret to other sections even in an organization and the data that is not ready for disclosure to other sections because it is being made, access can be limited only to users of a part of sections e. g. the section that makes the data, as shown in Table D (Fig. 6), thereby

causing security to be further improved.

[0078]

Also, in this embodiment, the contents of a page can be stored in the form of an easy-to-treat table on a relational database, as shown in Figs. 9 to 11, thereby causing the storage to be implemented easily.

[0079]

In other words, in this embodiment, setting of an access right to data can be implemented collectively by means of a superordinate concept of the kind of data and large classification, or using a part of data such as version and page as a unit. In addition, setting of an access right using these as a unit can be implemented based on a section or post.

[0080]

Consequently, sharing of information is easily compatible with security by disclosing an appropriate kind of data or an appropriate part of data to an appropriate post of person in a section concerned. In particular, in this embodiment, only when an access right to data is checked by the document making and reference right check unit in addition to the checking performed when to be logged in, which part of data such as version and page the data has is indicated by the document contents indication unit 44. Moreover, the page making and reference right check unit 45 checks the access right with regard to the part that a user is going to access and the kind of access. Thus, the security of the system is further improved by disclosing information to the user step by step.

[0081]

Enumerated as the concrete contents of a document in this embodiment is, for example, a document containing technical contents called a basic rule, a standard rule, or a standard plan. In such a document, each unified group like a specification of a product, standards of a product or handling regulations of a product is constituted as a logic page, and versions are increased each time the contents are revised, and versions both before and after revision are stored.

[0082]

By applying the present invention to such an example, it is possible to prevent the disclosure of unnecessary information, promote the sharing of information and improve security, for example, by disclosing a document or page of the most up-to-date version out of various documents to various sections and by limiting the persons who can access a document or page of older versions to the persons holding managerial posts.

[0083]

[5. Other embodiments] The present invention is not limited to the above-mentioned embodiment, but includes other embodiments exemplified as follows. In the above-mentioned embodiment, for example, a section and a post as organizational attributes are stored in the form of a code, but either a section or a post may be used. Also, whether a user has an access right or not can be judged based on an organizational attribute other than a section or a post such as a regular staff member, an external contracted employee and a temporary worker, and the attribute may be stored not by a code but by a character string e.g. "department manager" and "section manager."

[0084]

And the various tables described above can be decreased in number by increasing the number of items per table and integrating them, or, they can be disintegrated. In the above embodiment, the example in which each document is categorized into two ranks, a kind of document and large category, but documents can be categorized into three or more ranks.

[0085]

In the above-mentioned embodiment, whether a user has an access right or not is judged in two steps of the unit of documents and the unit of pages, but judgement can be collectively made once. Also, in the above-mentioned embodiment, indicated as the parts of data are three kinds of parts such as version of data, page included in data and version of page, but an access right does not necessarily need to be judged based on such divided parts, but only one or two kinds of parts can be introduced.

[0086]
Also, it is not mandatory to limit access only to users of a part of sections, and it is not mandatory either to store the contents of each page. Furthermore, for example, when a system itself is located in a safe place and no one other than authorized users can operate the system, the means or processing for checking whether a user has the right to use the database system is not mandatory either.

[0087]
[Effect of the invention] According to the present invention, an access right is correlated with the organizational attribute of a user, so that data management can be easily changed.

[Brief description of the drawings]
Fig. 1 is a conceptual diagram showing the outline of the present invention.
Fig. 2 is a block diagram showing the concrete configuration of the embodiment of the present invention.
Fig. 3 is a diagram showing the contents of Table A that collates document ID and the kind of document in the embodiment of the present invention.
Fig. 4 is a diagram showing the contents of Table B that collates document ID and a version in the embodiment of the present invention.
Fig. 5 is a diagram showing the contents of Table C that collates document ID and a logic page in the embodiment of the present invention.
Fig. 6 is a diagram showing the contents of Table D that collates a logic page and a secrecy level in the embodiment of the present invention.
Fig. 7 is a diagram showing the contents of Table E that collates the kind of document and a large classification in the embodiment of the present invention.
Fig. 8 is a diagram showing the contents of Table F that collates the kind of document and a logic page in the embodiment of the present invention.

Fig. 9 is a diagram showing the contents of Table G that collates a logic page and a table name in the embodiment of the present invention.
Fig. 10 is a diagram showing the contents of Tables TBL01 and TBL02 in the embodiment of the present invention.
Fig. 11 is a diagram showing the contents of Tables TBL31 and TBL32 in the embodiment of the present invention.
Fig. 12 is a diagram showing the contents of Document Reference Right Table that sets an access right related to reference using a document as a unit in the embodiment of the present invention.
Fig. 13 is a diagram showing the contents of Document Making Right Table that sets an access right related to making using a document as a unit in the embodiment of the present invention.
Fig. 14 is a diagram showing the contents of Page Reference Right Table that sets an access right related to reference using a page as a unit and Page Making Right Table that sets an access right related to making using a page as a unit in the embodiment of the present invention.
Fig. 15 is a diagram showing the contents of Table H that collates sections of each user with a user in the embodiment of the present invention.
Fig. 16 is a flowchart showing the processing procedures in the embodiment of the present invention.

[Explanations of letters or numerals]
1 Database
2 DBMS
3 Display input interface unit
3a Output device
3b Input device
4 Document management control unit
41 User check unit
42 Document access designation unit
142 Designation device
43 Document making and reference right check unit
143 Judgement device

44 Document contents indication unit

45 Page making and reference right check unit

46 Page indication and writing unit

146 Access device

H Attribute table

T Access right table

Fig. 1

H Attribute table

T Access right table

1 Database

142 Designation device

143 Judgement device

146 Access device

3a Output device

3b Input device

Fig. 2

3 Display input interface unit

4 Document management control unit

2 DBMS

1 Database

41 User check unit

42 Document access designation unit

43 Document making and reference right check unit

44 Document contents indication unit

45 Page making and reference right check unit

46 Page indication and writing unit

Fig. 3

Table A

Document ID	Kind of document	Document name	Symbol
A001	TS01	Product B	SA11
A002	MT02	Test method C	ZZk
A003	TS01	Product X	SAFF
A004	TS05	New product J	X-AK
A005	MT01	Manufacturing method F	T002
A006	TS05	New product V	X-BK
A007	MT01	Manufacturing method G	T356
A008	MT02	Test method K	ZFJ
:	:	:	:

Fig. 4

Table B

Document ID	Document ver	Issue date	Remarks
A001	1	Feb. 5, 1995	
A001	2	Mar. 1, 1997	
A002	1	May 8, 1995	
A003	1	Sep. 12, 1995	
A003	2	Jan. 20, 1996	
A003	3	May 30, 1997	
:	:	:	

Fig. 5

Table C

Document ID	Document ver	Logic page	Page ver
A001	1	PS01	1
A001	1	PS02	1
A001	1	PS03	1
A001	2	PS01	1
A001	2	PS02	2
A001	2	PS03	1
A002	1	PS01	1
A002	1	PS02	1
:	:	:	:

Fig. 6

Table D

Document ID	Logic page	Page ver	Secrecy level	Making section
A001	PS01	1		BUA01
A001	PS02	1		BUA01
A001	PS03	1	BUA02	BUA01
A001	PS02	2	J	BUA01
A002	PS01	1		BUA02
A002	PS02	1		BUA02
:	:	:		:

Fig. 7

Table E

Large classification	Kind of document
TS-A	TS01
TS-A	TS02
TS-A	TS03
TS-B	TS04
TS-B	TS05
	:
MT-A	MT01
MT-B	MT02
	:

Fig. 8

Table F

Kind of document	Logic page
TS01	PS01
TS01	PS02
TS01	PS03
TS02	PT01
TS02	PT02
TS03	PU01
TS03	PU02
TS03	PU03
:	
MT01	PM01
MT02	PF01
MT02	PF02
:	:

Fig. 9

Table G

Logic page	Table name
PS01	TBL01
PS01	TBL02
PS02	TBL11
:	:
PF01	TBL31
PF01	TBL32
:	:

Fig. 10

TBL01

Document ID	Page ver	Substance name	Quantity	Unit
A001	1	Covering agent	5	%
A001	1	Carbonate	8	%
A001	1	Activator	10	%
A001	1	perfume	1	%
A001	2	Covering agent	5	%
A001	2	Carbonate	9	%
A001	2	Activator	12	%
A001	2	Perfume	1	%
:	:	:	:	:

TBL02

Document ID	Page ver	Explanation
A001	1	··· of a cleaning agent
A001	2	A new composition ···
A003	1	Constituents of a plant ···
:	:	:

Fig. 11

TBL31

Document ID	Page ver	Device used	Explanation of test method	Remarks
A002	1	TYPE-A	Be careful of ···	
A008	1	TYPE-S	Sample ···	
A008	2	TYPE-S	Improved ···	
:	:	:	:	:

TBL32

Document ID	Page ver	File name
A002	1	DATA-010
A002	1	DATA-011
A008	1	DATA-020
A008	2	DATA-021
:	:	:

Fig. 12

Document reference table

Large classification	Kind of document	Section	Post
TS-A	TS01	BUA*	*
TS-A	TS02	*	A
TS-A	TS02	*	B
TS-A	TS03	BUG01	*
TS-A	TS03	BUG02	A
TS-A	TS03	BUG03	*
TS-B	*	*	*
:	:	:	:

Fig. 13

Document making Table

Large classification	Kind of document	Section	Post
TS-A	TS01	BUA01	*
TS-A	TS02	MUA02	A
TS-A	TS02	BUA02	B
TS-A	TS03	BUG01	*
TS-B	*	BUH03	*
:	:	:	:

Fig. 14

Page reference table

Logic page	Section	Post
PS01	*	B
PS01	*	A
PS02	*	*
PS03	BUA01	*
:	:	:

Page making table

Logic page	Section	Post
PS01	BUA01	A
PS01	BUA01	B
PS02	BUA01	B
PS03	BUA01	*
:	:	:

Fig. 15

Table H

Log-in name	password	Staff name	Section code	Post code
S9501234	XSDER	Taro Sato	BUA01	A
S9502368	TY2ERT	Ichiro Suzuki	BUA02	B
S9615236	55ERTY	Hanako Kobayashi	BUG01	A
S9825482	95DD522	Masao Yamamoto	BUA01	C
:	:	:	:	:

Fig. 16

Table H

Table A

Table E

Document making right table/Document reference right table

Table C/Table B

Page making right table/Page reference right table

Table D

TBL31, 32

TBL01, 02

Table G

Start

Step 1 Inputting log-in name and password

Step 2 Registered?

Step 3 Indicating a list of documents and designating a document

Step 4 Retrieving the kind of document

Step 5 Retrieving large classification

Step 6 Does the user have an access right?

Step 7 Indicating and designating document version, page and page version

Step 8 Does the user have an access right to the page?

Step 9 Is the secrecy level OK?

Step 10 Indicating document and accessing

End

Rejection of access

Continued from the front page
(72) Inventor: Toshikazu Ebata, c/o LION CORPORATION, 1-3-7, Honjo, Sumida-ku, Tokyo
(72) Inventor: Kazuhiko Saijo, c/o LION CORPORATION, 1-3-7, Honjo, Sumida-ku, Tokyo
(72) Inventor: Akihito Kobayashi, c/o CSK Co., Ltd., 2-6-1, Nishi-shinjuku, Shinjuku-ku, Tokyo
F-term (for reference)

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－20377
（P2000－20377A）
(43)公開日　平成12年１月21日(2000.1.21)

(51)Int.Cl.[7]		識別記号	FI			テーマコード（参考）
G06F	12/00	537	G06F	12/00	537A	5B017
	12/14	310		12/14	310K	5B082
	15/00	330		15/00	330D	5B085

審査請求　未請求　請求項の数18　ＯＬ　（全 14 頁）

(21)出願番号　特願平10－184434

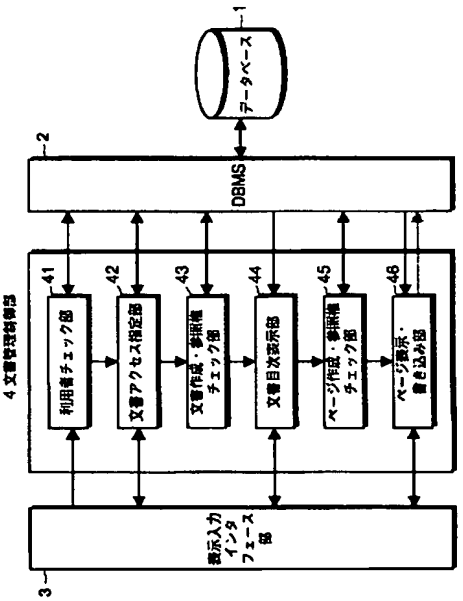
(22)出願日　平成10年６月30日(1998.6.30)

(71)出願人　000006769
ライオン株式会社
東京都墨田区本所１丁目３番７号
(71)出願人　000131201
株式会社シーエスケイ
東京都新宿区西新宿２丁目６番１号
(72)発明者　佐藤　豊之
東京都墨田区本所１丁目３番７号　ライオン株式会社内
(74)代理人　100081961
弁理士　木内　光春

最終頁に続く

(54)【発明の名称】　データベースシステム、データ管理方法及びデータ管理用ソフトウェアを記録した記録媒体

(57)【要約】
【課題】　アクセス権を、利用者の組織上の属性と関連づけることで容易に管理変更する。
【解決手段】　文書アクセス指定部４２によって、データベース１内のどの文書に対して、参照、作成、承認などといったどのようなモード（種類）のアクセスをするかを指定する。文書作成・参照権チェック部４３は、指定された文書とアクセスの種類に対して利用者がアクセス権を持つかどうか、利用者の部署及び役職に基づいて判断する。ページ作成・参照権チェック部４５は、文書目次表示部４４によって指定された部分とアクセスの種類に対して、利用者が参照、作成等を行なうアクセス権があるかどうかを調べる。ページ表示・書き込み部４６は、指定された文書のページを表示する。



1

【特許請求の範囲】
【請求項１】　データを管理するデータベースシステムにおいて、
どのデータにアクセスするか指定するための手段と、
指定されたデータへのアクセス権があるかどうかを、それぞれの利用者についてあらかじめ与えられた組織上の属性に基づいて判断する判断手段と、
アクセス権があると判断された利用者について、指定されたデータにアクセスさせるアクセス手段と、
を備えたことを特徴とするデータベースシステム。
【請求項２】　指定されたデータについてアクセス権があることが判断された場合に、
指定されたデータがどのような部分を持つかを表示する手段と、
データのどの部分にアクセスするか指定するための手段と、
指定された部分へのアクセス権があるかどうかを、それぞれの利用者についてあらかじめ与えられた組織上の属性について判断する第２の判断手段と、
を備え、
前記アクセス手段は、指定された部分へのアクセス権があると判断された利用者について、その部分にアクセスさせるように構成されたことを特徴とする請求項１記載のデータベースシステム。
【請求項３】　それぞれのデータをあらかじめ複数の分類に分けておき、
前記判断手段は、指定されたデータへのアクセス権があるかどうかを、指定されたデータの分類と、それぞれの利用者についてあらかじめ与えられた組織上の属性との関係に基づいて判断するように構成されたことを特徴とする請求項１又は２記載のデータベースシステム。
【請求項４】　データを管理するデータベースシステムにおいて、
利用者ごとに所属する部署と役職とを対応させるための属性テーブルと、
データを、１又は２以上のデータを含むデータ種類と、１又は２以上のデータ種類を含む大分類と、に分類するための分類テーブルと、
データごとに、１又は２以上のバージョンと、データに含まれるページ、ページごとの１又は２以上のバージョンのうち少なくとも１つを対応させるためのテーブルと、
データへのアクセス権があるかどうかを、前記データ種類、大分類、データ、データにかかわるバージョン、ページ、ページのバージョンのうち少なくとも１つごとに、前記部署又は役職のうち少なくとも一方に基づいて格納するためのアクセス権テーブルと、
を備えたことを特徴とするデータベースシステム。
【請求項５】　データを管理するデータベースシステムにおいて、

2

データ及びその部分ごとに、どのような組織上の属性を持つ利用者が、どのような種類のアクセスについてアクセス権を持つかを格納したアクセス権テーブルと、
利用者がデータベースシステムの利用権を持つかどうかをチェックする手段と、
アクセスしようとするデータを指定するための手段と、
指定されたデータに対して利用者がアクセス権を持つかどうかを、利用者の組織上の属性及び及び前記アクセス権テーブルに基づいて判断する手段と、
指定されたデータに対して利用者がアクセス権を持つとき、データがどのような部分を持つかを提示する手段と、
アクセスしようとする部分と、アクセスの種類とを指定するための手段と、
指定された部分とアクセスの種類について利用者がアクセス権を持つかどうかを前記アクセス権テーブルに基づいて判断する手段と、
指定された部分とアクセスの種類について利用者がアクセス権を持つとき、そのアクセスを実行させるアクセス手段と、
を備えたことを特徴とするデータベースシステム。
【請求項６】　データを管理するデータベースシステムにおいて、
それぞれの利用者の組織上の属性を格納する属性テーブルと、
それぞれのデータへのアクセス権があるかどうかを組織上の属性に基づいて格納するアクセス権テーブルと、
前記属性テーブルとアクセス権テーブルとに基づいて、指定されたデータへのアクセスを、個々の利用者に認めるかどうかを判断する判断手段と、
を備えたことを特徴とするデータベースシステム。
【請求項７】　個々のデータを１つ以上の階層を含む複数の分類に分ける分類テーブルを備え、
前記アクセス権テーブルは、データへのアクセス権があるかどうかを個々の分類に基づいて格納することを特徴とする請求項６記載のデータベースシステム。
【請求項８】　前記属性テーブルは、各利用者について部署及び役職のうち少なくとも一方を含み、
前記アクセス権テーブルは、データへのアクセス権があるかどうかを、部署及び役職のうち少なくとも一方に基づいて格納することを特徴とする請求項６又は７記載のデータベースシステム。
【請求項９】　前記アクセス権テーブルは、アクセス権があるかどうかを、アクセスの種類に応じて格納することを特徴とする請求項６から８のいずれか１つに記載のデータベースシステム。
【請求項１０】　前記アクセス権テーブルは、前記データのバージョン、データに含まれるページ、ページのバージョンのうち少なくとも１つを単位としてアクセス権があるかどうかを格納し、

前記判断手段は、データについて指定されたバージョン、ページ又はページのバージョンについてアクセスを認めるかどうかを判断するように構成されたことを特徴とする請求項６から９のいずれか１つに記載のデータベースシステム。

【請求項１１】　前記データ、データのバージョン、データのページ又はページのバージョンのうち少なくとも１つについて、一部の前記部署の利用者にだけアクセスを限定するためのテーブルを備えたことを特徴とする請求項６から１０のいずれか１つに記載のデータベースシステム。

【請求項１２】　データの内容を前記ページごとに格納するテーブルを備えたことを特徴とする請求項１０又は１１記載のデータベースシステム。

【請求項１３】　データを管理するデータ管理方法において、
どのデータにアクセスするか指定するためのステップと、
指定されたデータへのアクセス権があるかどうかを、それぞれの利用者についてあらかじめ与えられた組織上の属性に基づいて判断する判断のステップと、
アクセス権があると判断された利用者について、指定されたデータにアクセスさせるアクセスのステップと、
を含むことを特徴とするデータ管理方法。

【請求項１４】　指定されたデータについてアクセス権があると判断された場合に、
指定されたデータがどのような部分を持つかを表示するステップと、
データのどの部分にアクセスするか指定するためのステップと、
指定された部分へのアクセス権があるかどうかを、それぞれの利用者についてあらかじめ与えられた組織上の属性について判断する判断のステップと、を含み、
前記アクセスのステップは、指定された部分へのアクセス権があると判断された利用者について、その部分にアクセスさせることを特徴とする請求項１３記載のデータ管理方法。

【請求項１５】　それぞれのデータをあらかじめ複数の分類に分けておき、
前記判断のステップは、指定されたデータへのアクセス権があるかどうかを、指定されたデータの分類と、それぞれの利用者についてあらかじめ与えられた組織上の属性との関係に基づいて判断することを特徴とする請求項１３又は１４記載のデータ管理方法。

【請求項１６】　データを管理するデータ管理方法において、
利用者ごとに所属する部署と役職とを対応させるための属性テーブルと、
データを、１又は２以上のデータを含むデータ種類と、１又は２以上のデータ種類を含む大分類と、に分類するための分類テーブルと、
データごとに、１又は２以上のバージョンと、データに含まれるページ、ページごとの１又は２以上のバージョンのうち少なくとも１つを対応させるためのテーブルと、
データへのアクセス権があるかどうかを、前記データ種類、大分類、データ、データにかかわるバージョン、ページ、ページのバージョンのうち少なくとも１つごとに、前記部署又は役職のうち少なくとも一方に基づいて格納するためのアクセス権テーブルと、
を使うことを特徴とするデータ管理方法。

【請求項１７】　コンピュータを使ってデータを管理するためのデータ管理用ソフトウェアを記録した記録媒体において、
そのソフトウェアは前記コンピュータに、
どのデータにアクセスするかの指定を受け付けさせ、
指定されたデータへのアクセス権があるかどうかを、それぞれの利用者についてあらかじめ与えられた組織上の属性に基づいて判断させ、
アクセス権があると判断された利用者について、指定されたデータにアクセスさせることを特徴とするデータ管理用ソフトウェアを記録した記録媒体。

【請求項１８】　前記ソフトウェアは前記コンピュータに、
指定されたデータについてアクセス権があると判断された場合に、
指定されたデータがどのような部分を持つかを表示させ、
データのどの部分にアクセスするかの指定を受け付けさせ、
指定された部分へのアクセス権があるかどうかを、それぞれの利用者についてあらかじめ与えられた組織上の属性について判断させ、
指定された部分へのアクセス権があると判断された利用者について、その部分にアクセスさせることを特徴とする請求項１７記載のデータ管理用ソフトウェアを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、文書などのデータを格納して管理するデータベースシステムにかかわる技術の改良に関するもので、より具体的には、アクセス権を、利用者の組織上の属性と関連づけることで容易に管理変更するようにしたものである。

【０００２】

【従来の技術】複数の利用者が使うデータベースでは、文書、ファイル、データなど（以下「データ」と総称する）の不当な参照や改竄を防ぐため、アクセス権の管理が重要である。このアクセス権は、どの利用者がどのデータにどのようなアクセスができるかを表す権限であ

るデータ管理方法において、どのデータにアクセスするか指定するためのステップと、指定されたデータへのアクセス権があるかどうかを、それぞれの利用者についてあらかじめ与えられた組織上の属性に基づいて判断する判断のステップと、アクセス権があると判断された利用者について、指定されたデータにアクセスさせるアクセスのステップと、を含むことを特徴とする。請求項１７の発明は、請求項１，１３の発明を、コンピュータのソフトウェアを記録した記録媒体という見方からとらえたもので、コンピュータを使ってデータを管理するためのデータ管理用ソフトウェアを記録した記録媒体において、そのソフトウェアは前記コンピュータに、どのデータにアクセスするかの指定を受け付けさせ、指定されたデータへのアクセス権があるかどうかを、それぞれの利用者についてあらかじめ与えられた組織上の属性に基づいて判断させ、アクセス権があると判断された利用者について、指定されたデータにアクセスさせることを特徴とする。請求項１，６，１３，１７の発明では、利用者の部署や役職といった組織上の属性に基づいて、各データへのアクセスを認めるかどうか判断される。このため、異動などで部署や役職が変わる場合、組織上の属性を変更すればそれに伴ってアクセス権の内容も自動的に変わることになる。このため、アクセスするデータごとにパスワードを入力したり、異動のときにパスワードを変えたりデータごとのアクセス権を設定し直すといった煩わしい手数が不要になる。

【００１４】請求項２の発明は、請求項１記載のデータベースシステムにおいて、指定されたデータについてアクセス権があると判断された場合に、指定されたデータがどのような部分を持つかを表示する手段と、データのどの部分にアクセスするか指定するための手段と、指定された部分へのアクセス権があるかどうかを、それぞれの利用者についてあらかじめ与えられた組織上の属性について判断する第２の判断手段と、を備え、前記アクセス手段は、指定された部分へのアクセス権があると判断された利用者について、その部分にアクセスさせるように構成されたことを特徴とする。請求項５の発明は、データを管理するデータベースシステムにおいて、データ及びその部分ごとに、どのような組織上の属性を持つ利用者が、どのような種類のアクセスについてアクセス権を持つかを格納したアクセス権テーブルと、利用者がデータベースシステムの利用権を持つかどうかをチェックする手段と、アクセスしようとするデータを指定するための手段と、指定されたデータに対して利用者がアクセス権を持つかどうかを、利用者の組織上の属性及び及び前記アクセス権テーブルに基づいて判断する手段と、指定されたデータに対して利用者がアクセス権を持つとき、データがどのような部分を持つかを提示する手段と、アクセスしようとする部分と、アクセスの種類とを指定するための手段と、指定された部分とアクセスの種類について利用者がアクセス権を持つかどうかを前記アクセス権テーブルに基づいて判断する手段と、指定された部分とアクセスの種類について利用者がアクセス権を持つとき、そのアクセスを実行させるアクセス手段と、を備えたことを特徴とする。請求項１４の発明は、請求項２の発明を方法という見方からとらえたもので、請求項１３記載のデータ管理方法において、指定されたデータについてアクセス権があると判断された場合に、指定されたデータがどのような部分を持つかを表示するステップと、データのどの部分にアクセスするか指定するためのステップと、指定された部分へのアクセス権があるかどうかを、それぞれの利用者についてあらかじめ与えられた組織上の属性について判断する判断のステップと、を含み、前記アクセスのステップは、指定された部分へのアクセス権があると判断された利用者について、その部分にアクセスさせることを特徴とする。請求項１８の発明は、請求項２，１４の発明を、コンピュータのソフトウェアを記録した記録媒体という見方からとらえたもので、請求項１７記載のデータベースシステムにおいて、前記ソフトウェアは前記コンピュータに、指定されたデータについてアクセス権があると判断された場合に、指定されたデータがどのような部分を持つかを表示させ、データのどの部分にアクセスするかの指定を受け付けさせ、指定された部分へのアクセス権があるかどうかを、それぞれの利用者についてあらかじめ与えられた組織上の属性について判断させ、指定された部分へのアクセス権があると判断された利用者について、その部分にアクセスさせることを特徴とする。請求項２，５，１４，１８の発明では、ログイン時のチェックに加え、データに対するアクセス権が確認できたときだけ、データがバージョンやページといったどのような部分を持つかが提示される。そしてさらに、アクセスしようとする部分とアクセスの種類についてもアクセス権の確認を行う。このように、利用者に対して段階的に情報を開示することで、システムのセキュリティが一層向上する。

【００１５】請求項３の発明は、請求項１又は２記載のデータベースシステムにおいて、それぞれのデータをあらかじめ複数の分類に分けておき、前記判断手段は、指定されたデータへのアクセス権があるかどうかを、指定されたデータの分類と、それぞれの利用者についてあらかじめ与えられた組織上の属性との関係に基づいて判断するように構成されたことを特徴とする。請求項７の発明は、請求項３の発明に関連して、テーブルというデータ構造を示したもので、請求項６記載のデータベースシステムにおいて、個々のデータを１つ以上の階層を含む複数の分類に分ける分類テーブルを備え、前記アクセス権テーブルは、データへのアクセス権があるかどうかを個々の分類に基づいて格納することを特徴とする。請求項１５の発明は、請求項３の発明を方法という見方からとらえたもので、請求項１３又は１４記載のデータ管理

り、一般に、作成、参照、編集、承認、削除など、アクセスの種類別に設定される。

【０００３】このようなアクセス権の管理にかかわる技術としては、

（１）まず、データを単位としてキーワードやアクセスコードなどのパスワードを設定し、そのパスワードを知っている利用者に、そのファイルへのアクセスを許すものが知られている。

【０００４】（２）また、ディレクトリなどを単位としたデータの集合体を単位としてアクセス権を設定し、利用者が入力した利用者ＩＤとパスワードに基づいて、どの集合体へのアクセスを認めるかを制限する例も知られている。

【０００５】（３）さらに、特開平９－６６８１に開示されているように、利用者がある一群のデータにアクセスする際、どの項目を操作できるか、また、どのような内容の操作を認めるかといった複数種類の権限について可否を設定するとともに、個々の利用者ごとに、それぞれのデータ群にかかわるそのような権限の種類を割り付けることができる例も知られている。

【０００６】（４）また、特許２７００５１７（特開平６－２６６５９１）では、リレーショナルデータベースを使ったデータ管理について、データの各バージョンやデータのページ単位の各バージョン同士を、互いに関連づけて同時に格納しておく例が開示されている。この例では、さらに、それら各バージョンやページに機密種類を設定し、利用者ごとの属性に基づいてアクセス権を管理することができる。

【０００７】

【発明が解決しようとする課題】しかしながら、上に述べたような従来技術では、組織上の部署や役職とは別個独立に、アクセス権を個々の利用者単位に管理していたため、データの種類が増えたり人事異動などがあると、アクセス権にかかわる変更が煩わしいという問題があった。

【０００８】すなわち、上に述べた（１）の例では、データを対象としてパスワードが設定されるため、そのデータを使って共通の業務を行なう個々の利用者がパスワードを教えてもらわなくてはデータを使用できなかった。このため、必要な範囲の利用者にパスワードを知らせる手数がかかり、また、パスワードの種類が増えるため利用者の側でもパスワードを管理する負担が多いという問題があった。また、パスワードを知っている利用者が異動などでデータに対するアクセス権を失ったときは、パスワードを変更するなどの煩雑な手数が必要であった。

【０００９】また、上に述べた（２）の例では、集合体に対応するＩＤとパスワードを、アクセス可能な個々の利用者に対してのみわかるようにしなければならず、異動などで仕事が変わったりしてアクセス権を消失するような場合、もとのアクセス権者による無権限なアクセスを防ぐといった管理が難しかった。

【００１０】さらに、上に述べた（３）の例では、個々の利用者と、操作できる項目や内容との関係で権限を設定するため、アクセス権の設定が複雑であった。特に、会社での部署の移動などで利用者の仕事が変化し、アクセス権が変化するような場合、上に述べたような個々の利用者と項目や内容との関係でアクセス権を再設定しなければならず、その手数が負担になるという問題があった。

【００１１】特に、会社のような組織内でのアクセス権については、どの程度の役職の利用者ならアクセスしてよいかという観点と、どの部署の利用者にアクセスを認めれば合理的かという観点が両方必要である。しかし、従来は、このように本来複数あるべき観点を、アクセス権を表すテーブルに一元化していた。このため、人の異動があったり、事業部の再編があったり、データが増えたような場合、このような一元的なテーブルを個々人との関係で矛盾がないように修正しなければならず、正しく修正するには煩雑な手数がかかるという問題もあった。

【００１２】この発明は、上に述べたような従来技術の問題点を解決するために提案されたもので、その目的は、アクセス権を、利用者の組織上の属性と関連づけることで容易に管理変更することである。また、この発明の他の目的は、複数の文書についてアクセス権をまとめて効率良く設定することである。また、この発明の他の目的は、文書の部分ごとにアクセス権を設定できるようにすることで、セキュリティをきめ細かく管理することである。

【００１３】

【課題を解決するための手段】上に述べた目的を達成するため、請求項１の発明は、データを管理するデータベースシステムにおいて、どのデータにアクセスするか指定するための手段と、指定されたデータへのアクセス権があるかどうかを、それぞれの利用者についてあらかじめ与えられた組織上の属性に基づいて判断する判断手段と、アクセス権があると判断された利用者について、指定されたデータにアクセスさせるアクセス手段と、を備えたことを特徴とする。請求項６の発明は、請求項１の発明に関連して、テーブルというデータ構造を示したもので、データを管理するデータベースシステムにおいて、それぞれの利用者の組織上の属性を格納する属性テーブルと、それぞれのデータへのアクセス権があるかどうかを組織上の属性に基づいて格納するアクセス権テーブルと、前記属性テーブルとアクセス権テーブルとに基づいて、指定されたデータへのアクセスを、個々の利用者に認めるかどうかを判断する判断手段と、を備えたことを特徴とする。請求項１３の発明は、請求項１の発明を方法という見方からとらえたもので、データを管理す

方法において、それぞれのデータをあらかじめ複数の分類に分けておき、前記判断のステップは、指定されたデータへのアクセス権があるかどうかを、指定されたデータの分類と、それぞれの利用者についてあらかじめ与えられた組織上の属性との関係に基づいて判断することを特徴とする。請求項３，７，１５の発明では、データの種類やさらに上位の大分類といった上位概念を使って、性質の共通する複数のデータについてアクセス権をまとめて効率よく設定することができる。

【００１６】請求項４の発明は、データを管理するデータベースシステムにおいて、利用者ごとに所属する部署と役職とを対応付けるための属性テーブルと、データを、１又は２以上のデータを含むデータ種類と、１又は２以上のデータ種類を含む大分類と、に分類するための分類テーブルと、データごとに、１又は２以上のバージョンと、データに含まれるページ、ページごとの１又は２以上のバージョンのうち少なくとも１つを対応させるためのテーブルと、データへのアクセス権があるかどうかを、前記データ種類、大分類、データ、データにかかわるバージョン、ページ、ページのバージョンのうち少なくとも１つごとに、前記部署又は役職のうち少なくとも一方に基づいて格納するためのアクセス権テーブルと、を備えたことを特徴とする。請求項１６の発明は、請求項４の発明を方法という見方からとらえたもので、データを管理するデータ管理方法において、利用者ごとに所属する部署と役職とをあらかじめ対応付けておき、データを、１又は２以上のデータを含むデータ種類と、１又は２以上のデータ種類を含む大分類と、に分類しておき、データごとに、１又は２以上のバージョンと、データに含まれるページ、ページごとの１又は２以上のバージョンのうち少なくとも１つを対応させておき、データへのアクセス権があるかどうかを、前記データ種類、大分類、データ、データにかかわるバージョン、ページ、ページのバージョンのうち少なくとも１つごとに、前記部署又は役職のうち少なくとも一方に基づいて判断することを特徴とする。請求項４，１６の発明では、データに対するアクセス権の設定を、データ種類や大分類といった上位概念でまとめて行うこともできるし、バージョンごとやページごとといったデータの部分を単位として行うこともできる。しかも、それらを単位としたアクセス権の設定を、部署や役職に基づいて行うことができる。このため、適切な種類のデータやデータの適切な部分を、関係のある部署のしかるべき役職者に公開することで、情報の共有とセキュリティを容易に両立することができる。なお、これら各テーブルを使った処理手順としては、例えば、まずデータを単位としてアクセス権を確認すると、どのようなバージョンやページがあるか見ることができ、次にそれに基づいて、アクセスしようとするバージョンやページをさらに選ぶと、選んだバージョンやページについて具体的なアクセス権が確認される、といったものが考えられる。また、各テーブルはそれぞれ単一のテーブルとして構成してもよいし、例えば対応関係の種類ごとに複数のテーブルとして構成してもよい。

【００１７】請求項８の発明は、請求項６又は７記載のデータベースシステムにおいて、前記属性テーブルは、各利用者について部署及び役職のうち少なくとも一方を含み、前記アクセス権テーブルは、データへのアクセス権があるかどうかを、部署及び役職のうち少なくとも一方に基づいて格納することを特徴とする。請求項８の発明では、部署や役職に基づいてアクセス権の有無を判断するので、部署ごとに系統化され階層的な役職制度を持つ多くの組織に適用することが容易である。

【００１８】請求項９の発明は、請求項６から８のいずれか１つに記載のデータベースシステムにおいて、前記アクセス権テーブルは、アクセス権があるかどうかを、アクセスの種類に応じて格納することを特徴とする。請求項９の発明では、データを見るだけの参照、データの作成、データの内容の承認といったアクセスの種類に応じてアクセス権を設定できるので、業務の流れや権限の範囲に応じてセキュリティをきめ細かく管理することができる。

【００１９】請求項１０の発明は、請求項６から９のいずれか１つに記載のデータベースシステムにおいて、前記アクセス権テーブルは、前記データのバージョン、データに含まれるページ、ページのバージョンのうち少なくとも１つを単位としてアクセス権があるかどうかを格納し、前記判断手段は、データについて指定されたバージョン、ページ又はページのバージョンについてアクセスを認めるかどうかを判断するように構成されたことを特徴とする。請求項１０の発明では、文書などのデータについて、バージョンごとやページごといった部分を単位にアクセス権を設定できる。このため、１つのデータでも部分によって性質が違う場合、アクセスを認めるかどうかを無理にデータ全体として決める必要がない。これによって、部分の性質に応じて、アクセスを認めて情報の利用を優先するか、アクセスを認めずにセキュリティを優先するかをきめ細かく設定することが可能となる。

【００２０】請求項１１の発明は、請求項６から１０のいずれか１つに記載のデータベースシステムにおいて、前記データ、データのバージョン、データのページ又はページのバージョンのうち少なくとも１つについて、一部の前記部署の利用者にだけアクセスを限定するためのテーブルを備えたことを特徴とする。請求項１１の発明では、組織の内部でも他の部署には秘密にしなければならない機密事項にかかわるデータや、作成途中であるため他の部署に公開する段階にないデータなどについて、そのデータを作成した部署など一部の部署の利用者だけにアクセスを限定することができ、セキュリティが一層

向上する。

【００２１】請求項１２の発明は、請求項１０又は１１記載のデータベースシステムにおいて、データの内容を前記ページごとに格納するテーブルを備えたことを特徴とする。請求項１２の発明では、ページの内容についても、リレーショナルデータベース上で扱いやすいテーブル形式で格納するので、実装が容易になる。

【００２２】

【発明の実施の形態】以下、この発明の実施の形態（以下「実施形態」という）について図面を参照しながら説明する。なお、この発明は、周辺機器を持つコンピュータを、ソフトウェアで制御することによって実現されることが一般的と考えられる。この場合、そのソフトウェアは、この明細書の記載にしたがった命令を組み合わせることで作られ、上に述べた従来技術と共通の部分には従来技術で説明した手法も使われる。また、そのソフトウェアは、プログラムコードだけでなく、プログラムコードの実行のときに使うために予め用意されたデータも含む。

【００２３】そして、そのソフトウェアは、ＣＰＵ、コプロセッサ、各種チップセットといった処理装置、キーボードやマウスといった入力装置、メモリやハードディスク装置といった記憶装置、ディスプレイやプリンタといった出力装置などの物理的な資源を活用することでこの発明の作用効果を実現する。

【００２４】但し、この発明を実現する具体的なソフトウェアやハードウェアの構成はいろいろ変更することができる。例えば、ソフトウェアの形式には、コンパイラ、インタプリタ、アセンブラなどいろいろあり、外部との情報をやり取りするにも、フロッピーディスクなどの着脱可能な記録媒体、ネットワーク接続装置などいろいろ考えられる。また、この発明を実現するソフトウェアやプログラムを記録したＣＤ－ＲＯＭのような記録媒体は、単独でもこの発明の一態様である。さらに、この発明の機能の一部をＬＳＩなどの物理的な電子回路で実現することも可能である。

【００２５】以上のように、コンピュータを使ってこの発明を実現する態様はいろいろ考えられるので、以下では、この発明や実施形態に含まれる個々の機能を実現する仮想的回路ブロックを使って、この発明と実施形態とを説明する。なお、説明で使うそれぞれの図について、それ以前の図で説明したものと同じ要素や同じ種類の要素については同じ符号を付け、説明は省略する。

【００２６】〔１．実施形態の概略〕まず、図１は、この実施形態の概略を示す概念図である。すなわち、この実施形態では、図１に示すように、データベース１に文書などのデータを格納しておき、属性テーブルＨには、利用者ごとの部署や役職といった属性を格納しておき、アクセス権テーブルＴには、データベース１に格納された個々の文書について、どのような属性の利用者であれば参照や作成にかかわるアクセス権を持つかを格納しておく。また、利用者との間で指示やデータなどの情報をやり取りするインタフェースとして、ＣＲＴモニタなどの出力手段３ａや、キーボードやマウスといった入力手段３ｂとを設ける。

【００２７】そして、利用者が、アクセスしたい文書を指定手段１４２から指定すると、判断手段１４３が、上に述べた属性テーブルＨとアクセス権テーブルＴとを参照することで、その利用者の組織上の属性に基づいて、指定された文書に対するアクセス権を持つかどうか判断する。そして、利用者がアクセス権を持つときは、指定された文書へのアクセスを、アクセス手段１４６が実行する。

【００２８】〔２．実施形態の構成〕

〔２－１．全体の構成〕次に、図２は、この実施形態の具体的な構成を示す機能ブロック図である。すなわち、この実施形態は、この発明をリレーショナルデータベースに適用したもので、図２に示すように、データベース１と、ＤＢＭＳ（データベース管理システム）２と、表示入力インターフェース部３と、文書管理制御部４と、を備えている。

【００２９】このうち、データベース１は、リレーショナルデータベースで、いろいろなデータをテーブル（表）形式で格納することができる。また、データベース１には、文字列テキストのような文書だけでなく、各種アプリケーションプログラム特有の修飾データを含むファイル、ビットマップイメージなどの画像ファイル、表計算プログラム用のワークシート、ドローツールやグラフィックソフト用の図面データファイルなどいろいろな種類のファイルをデータとして格納することができる。

【００３０】但し、ここでは、データベース１はデータとして文書を格納し、また、後に具体的に説明するが、文書を管理したり文書に対するアクセス権を管理するための複数のテーブルも格納しているものとする。

【００３１】また、ＤＢＭＳ２は、データベース１に格納された文書などのデータに対して、作成、追加、検索、更新、削除といったいろいろな操作を行う部分である。また、表示入力インターフェース部３は、利用者からいろいろな指示やデータの入力を受け付けたり、利用者に対してデータベース１から取り出されたデータや操作上のプロンプトなどのメッセージといった情報を提示するインタフェースである。

【００３２】また、文書管理制御部４は、表示入力インターフェース部３を通して与えられる利用者からの指示にしたがって、データベース１中の各テーブルを参照しながら、アクセス権のある利用者に対してデータベース１中の文書にアクセスさせる部分である。この文書管理制御部４は、具体的には、利用者チェック部４１と、文書アクセス指定部４２と、文書作成・参照権チェック部

４３と、文書目次表示部４４と、ページ作成・参照権チェック部４５と、ページ表示・書き込み部４６と、を備えている。

【００３３】このうち、利用者チェック部４１は、表示入力インターフェース部３から入力された個人のＩＤやパスワードなどに基づいて、データベース１にアクセスしようとしている利用者が、登録された正規の利用者かどうかをチェックすると共に、その利用者について所属や役職といった組織上の属性を、アクセス権のチェックに使うためにデータベース１内のテーブルから取り込む手段である。

【００３４】また、文書アクセス指定部４２は、利用者がデータベース１内のどの文書に対して、参照、作成、承認などといったどのようなモード（種類）のアクセスをするかを指定する手段であり、文書アクセス指定部４２は、このように指定された文書について、データベース１内のテーブルから、どの文書であるかを一義的に規定するための文書のＩＤ番号を取得する。

【００３５】また、文書作成・参照権チェック部４３は、指定された文書に対して利用者が参照や作成、承認等を行なう権利、すなわちアクセス権があるかどうかを調べる手段であり、このアクセス権がなければ目次の表示といった次の段階へは進めない。

【００３６】また、文書目次表示部４４は、指定された文書がどのようなバージョンやどのような論理的なページ（論理ページ又はページと呼ぶ）を持っているかといった構成（目次と呼ぶ）を、表形式で表示する手段である。そして、利用者はこの目次を見て、どの部分、すなわちどのバージョンやどのページについてアクセスしたいかを文書目次表示部４４に対して指定し、また、アクセスの種類として参照モードや作成モードといったモードを指定する。

【００３７】また、ページ作成・参照権チェック部４５は、文書目次表示部４４によって指定された部分とアクセスの種類に対して、利用者が参照、作成等を行なうアクセス権があるかどうかを調べる手段であり、アクセス権がなければ次の段階へは進めない。なお、文書作成・参照権チェック部４３とページ作成・参照権チェック部４５とは、指定されたデータへのアクセスを、個々の利用者に認めるかどうかを判断するもので、特許請求の範囲にいう判断手段にあたり、特に、ページ作成・参照権チェック部４５は、特許請求の範囲にいう第２の判断手段にあたる。

【００３８】また、ページ表示・書き込み部４６は、指定された文書のページを表示する手段である。そして、このページ表示・書き込み部４６では、文書を作成モードで開いた場合は表示画面内でその文書に対して書き込んだり書き換えたりが可能であり、書き込んだ内容はデータベース１に登録することが可能である。一方、ページ表示・書き込み部４６においても、文書を参照モードで開いた場合は、文書の書き込みや書き換えはできない。このページ表示・書き込み部４６は、特許請求の範囲にいうアクセス手段にあたる。

【００３９】〔２－２．テーブルの構成〕また、データベース１には、文書管理とアクセス権の管理を行なうために必要な以下のテーブルが登録されている。まず、図３に示すテーブルＡは、個々の文書について、名称、記号と文書種類を格納したテーブルである。また、このテーブルＡでは、各文書に対して、文書間で互いに重複しないように一義的に付与されたユニークな文書ＩＤと、その文書がどの文書種類に属しているかが登録されている。なお、文書は互いに文書ＩＤによって識別されるので、文書名はユニーク（唯一的）でなくてもよく、文書の用途に応じて自由に名付けることができる。

【００４０】また、図４に示すテーブルＢは、文書ＩＤで特定される文書ごとに、文書全体としていくつのどのようなバージョン（文書Ｖｅｒ）のものが発行され格納されているかを表すものである。例えば文書ＩＤが「Ａ００１」の文書としては、互いに違った日付で作成されたバージョン１と２という２つのバージョンのものがある。

【００４１】また、図５に示すテーブルＣは、図４に示したテーブルＢにおいて文書ＩＤで特定される文書の個々のバージョンが、どのような論理ページでできているかを格納していて、さらに、それら個々のページが、どのようなバージョン（ページバージョンと呼ぶ）を持っているかを表している。

【００４２】また、図６に示すテーブルＤは、図５に示したテーブルＣで、各文書を構成するものとされる個々の論理ページやそのページバージョンについて、どの部署によって作成されたか（作成部署）と、アクセス権を一部の部署に限定する情報である機密レベルが対応付けられている。

【００４３】また、図７に示すテーブルＥは、図３に示したテーブルＡで各文書に対応付けられた文書種類を、さらに上位概念である大分類に分類している。これによって、後に詳しく説明するが、大分類という上位概念を単位として作成や参照をするためのアクセス権を容易に設定することが可能になる。なお、図３に示したテーブルＡとこのテーブルＥとは、個々の文書を２つの階層で分類するものであり、上に述べた分類テーブルにあたる。

【００４４】また、図８に示すテーブルＦは、文書種類ごとに、どのような論理ページを含むべきかという対応関係を表わしていて、文書を新規に作成するときなどこのテーブルを参照することで必要なページが構成される。

【００４５】また、上に述べた個々の論理ページの内容は別のテーブルに格納されていて、図９に示すテーブルＧは、このように各論理ページごとの内容がどのテーブ

ルに格納されているかを表している。このように、個々の論理ページの内容をテーブルに格納することで、データ自体とデータ管理用のテーブルとを、リレーショナルデータベース上で取り扱うことのできる同じテーブル形式で構成できるので、実装が容易になる。

【００４６】また、図１０に示すテーブルＴＢＬ０１，ＴＢＬ０２は、図９のテーブルＧで示したように、論理ページＰＳ０１を構成している（図９）実際のデータを、データの性質に応じて２つに分けてそれぞれ格納しているテーブルである。同じように、図１１に示すテーブルＴＢＬ３１，ＴＢＬ３２は、別のある論理ページＰＦ０１を構成している（図９）実際のデータを格納しているテーブルである。なお、これらページの内容は、具体的な文書の用途や使用するアプリケーションプログラムに応じて異なるので、一定の形式（フォーマット）に限定する必要はなく、自由に定めることができる。

【００４７】また、図１２に示す文書参照権テーブルは、文書の大分類や文書種類に基づいて、どのような部署又は役職の利用者であれば、参照モードでアクセスするためのアクセス権があるかが登録されているテーブルである。同じように、図１３に示す文書作成権テーブルは、文書の大分類や文書種類ごとに、どのような部署又は役職の利用者であれば、作成モードでアクセスするためのアクセス権があるかが登録されているテーブルである。

【００４８】また、図１４に示すページ参照権テーブルは、文書の論理ページごとに、どのような部署又は役職の利用者であれば、参照モードでアクセスするためのアクセス権があるかが登録されているテーブルであり、同じ図１４に示すページ作成権テーブルは、文書の論理ページごとに、どのような部署又は役職の利用者であれば、作成モードでアクセスするためのアクセス権があるかが登録されているテーブルである。

【００４９】なお、図１２～１４に示す各テーブルは、データへのアクセス権があるかどうかを部署、役職といった組織上の属性に基づいて格納するもので、上に述べたアクセス権テーブルにあたる。また、これらアクセス権テーブルは、個々のテーブルについて上に説明したように、アクセス権があるかどうかを、アクセスの種類ごとに格納している。

【００５０】特に、図１４に示したページ参照権テーブル及びページ作成権テーブルは、データに含まれるページごとにアクセス権を設定しているが、アクセス権テーブルには、文書のバージョンごとや、ページのバージョンごとにアクセス権を設定しておくこともできる。

【００５１】また、図１５に示すテーブルＨは、システムを使用する個々の利用者にかかわる情報を格納しているテーブルであり、具体的には、利用者が登録されている正規の利用者かどうか確認するためのログイン名、パスワードの他、アクセス権の判断に使うために、所属している部署の部署コード、役職を表す役職コードなどを含んでいる。これら部署や役職は、利用者の組織上の属性であり、このテーブルＨは上に述べた属性テーブルにあたる。

【００５２】〔３．実施形態の作用〕上に述べたように構成されたこの実施形態は、次のように作用する。ここで、図１６は、この実施形態における処理手順を示すフローチャートである。

〔３－１．利用者認証と文書指定〕まず、利用者は、表示入力インターフェース部３から自分のログイン名とパスワードを入力する（ステップ１）。このように利用者にかかわるデータが入力されると、文書管理制御部４では利用者チェック部４１が起動し、この利用者チェック部４１は、ＤＢＭＳ２を通してデータベース１内のテーブルＨ（図１５）にアクセスし、入力されたログイン名やパスワードに該当する利用者が登録されているかをチェックする。

【００５３】その結果、該当する利用者が登録されていれば（ステップ２）、利用者チェック部４１は、ログインした利用者の部署コードと役職コードとをテーブルＨから読み出して文書管理制御部４内に保存し、文書アクセス指定部４２を起動する。

【００５４】このようにログインに成功すると、文書アクセス指定部４２は、データベース１内にどのような文書が格納されているかを、データベース１内のテーブルＡ（図３）に基づいて表示入力インターフェース部３に表示画面に一覧表示し、利用者は、このように表示された文書の一覧などから自分がアクセスしたい文書を指定する（ステップ３）。この指定では、どの文書を見たいかを文書ＩＤで特定し、その文書に対して利用者がただ単に参照したいだけなのか（参照モード）、編集もしたいか（作成モード）を特定する。

【００５５】なお、文書を具体的にどのような形式で表示するかは自由であり、改めて図示はしないが、例えば文書の名称順、最終更新日付順などに基づいて単純に一覧表示してもよいし、例えば文書の種類ごとやディレクトリごとにツリー表示してもよいし、アクセス権のレベル別などに表示してもよい。

【００５６】〔３－２．文書単位のアクセス権の判断〕続いて、文書アクセス指定部４２は、指定された文書の文書ＩＤに基づいて、データベース１内のテーブルＡ（図３）を検索することで、指定された文書に相当する文書種類を特定し（ステップ４）、さらに、データベース１内のテーブルＥ（図７）を検索することで、その文書種類に対応する大分類を取得する（ステップ５）。

【００５７】次に、文書管理制御部４の文書作成・参照権チェック部４３は、このように取得したその文書種類と大分類と、テーブルＨから得られた利用者の部署及び役職とを、データベース１内の文書参照権テーブル（図１２）及び文書作成権テーブル（図１３）と照らし合わ

せることで、その利用者が指定された文書を参照したり作成するためのアクセス権を持つかどうかを調べる（ステップ６）。

【００５８】例えば、図１２に示した文書参照権テーブルを例にとってどのようにアクセス権が設定されているかを説明すると、

（１）文書種類ＴＳ０１については、部署コードの先頭３文字がＢＵＡである利用者には、参照権がある。

（２）また、文書種類ＴＳ０２については、どのような部署の利用者かを問わず、役職がＡ又はＢであれば参照権がある。

（３）また、大分類ＴＳ－Ｂに属する文書、例えば文書種類ＴＳ０４やＴＳ０５の文書については、文書の種類を問わず、どの部署のどの役職の利用者でも参照権がある。

なお、これら文書参照権テーブル（図１２）や文書作成権テーブル（図１３）中の「＊」印（アスタリスク）は、その項目については限定がないこと、すなわちいわゆるワイルドカードを表わしている。ステップ６におけるこのようなチェックでアクセス権ありと判断されると、次の文書目次表示部４４が起動される。

【００５９】〔３－３．ページ単位のアクセス権の判断〕文書目次表示部４４は、利用者から指定された文書の文書ＩＤに基づいて、データベース１内のテーブルＡ，Ｂ，Ｃ，Ｄ（図３～６）を検索することで、その文書がどのようなバージョン、ページ、ページのバージョンといった部分からできているかを表す情報を取得し、これらの情報に基づいて指定された文書にどのようなバージョン、ページやページのバージョンがあるか及び各々の機密レベル、作成部署を表示する（ステップ７）。

【００６０】そして、利用者はこの表示に基づいて、どのページやバージョンといった部分についてアクセスしたいか、また、参照、作成といったどのようなモードでアクセスしたいか、すなわちアクセスの種類を指定する（ステップ７）。ここでは、利用者が論理ページに基づいてアクセスの対象を指定したものとする。

【００６１】すると、次にページ作成・参照チェック部４５は、さらに、このように指定された部分及びアクセスの種類に対して、利用者が作成権や参照権を持っているかをページ参照権テーブル、ページ作成権テーブル（図１４）を検索することによって調べる（ステップ８）。ここで、これらページ参照権テーブルやページ作成権テーブルの中で、アクセス権がどのような形式で設定されているかは、文書参照権テーブル（図１２）について上で説明したものと同様である。

【００６２】さらに、ページ作成・参照権チェック部４５は、指定された論理ページの指定ページバージョンについて、データベース１内のテーブルＤ（図６）に格納された機密レベルを参照する（ステップ９）。この機密レベルという項目は、個々の文書の論理ページに対してのアクセス権を、一部の部署や役職に一時的に限定するもので、例えば、図６で「Ｊ」と設定されている論理ページに対しては、その論理ページの作成部署として登録されている部署の利用者以外は参照、作成できない。

【００６３】また、上に述べた「Ｊ」以外の例えば「ＢＵＡ０２」（図６）のように部署コードが設定されている場合は、設定されたコードと同じ部署又は作成部署以外は参照、作成できないことを示している。なお、ここではデータのページとそのバージョンについて機密レベルを設定する例を示したが、機密レベルは、文書全体や文書のバージョンを単位として設定してもよい。

【００６４】〔３－４．ページへのアクセス〕そして、上に述べたような全てのチェックでアクセス権ありと判断された場合のみ、ページ表示・書き込み部４６によって、利用者の指定したページの実体が表示され、利用者が指定したアクセスの種類に応じて、参照することだけ可能となったり、内容を編集することも可能な状態となる（ステップ１０）。一方、ステップ２，６，８又は９のいずれかのチェックでアクセス権がないなどの判断がされるとアクセスは拒否される。

【００６５】具体的には、ページ表示・書き込み部４６は、指定された論理ページに対応するデータがどのテーブルに格納されているかのテーブル名を、データベース１内のテーブルＧ（図９）から検索し、それによって判明したテーブル名を持つテーブル、例えばテーブルＴＢＬ０１，ＴＢＬ０２（図１０）、テーブルＴＢＬ３１，ＴＢＬ３２（図１１）などから、指定された文書ＩＤと論理ページに対応するデータを取得して表示する。

【００６６】例えば、テーブルＧを参照する結果、論理ページＰＳ０１の内容を表すデータはテーブルＴＢＬ０１，ＴＢＬ０２に入っていることが判明するので、これらおのおののテーブルＴＢＬ０１，ＴＢＬ０２から、該当する文書ＩＤ例えばＡ００１のデータを検索することで、利用者の指定したページのデータを取得し、表示入力インターフェース部３に表示できることになる。

【００６７】そして、利用者がその論理ページに対するアクセスの種類として「作成」モードを指定していた場合は、例えば表示画面上の編集可能な文字列の部分に点滅するカーソルが現われ、利用者がそのカーソルを使って内容を編集し、終了の操作をすると、このように編集された内容が再び対応するテーブルに書き戻されることで、データベース１内の文書が更新される。

【００６８】また、このような作成によって、文書の新しいバージョンや、新しい論理ページ、論理ページの新しいバージョンといった部分が作られると、それに応じてテーブルＢ，Ｃなどが更新され、新しく作られた部分は、しかるべきテーブルに追加され、その後のアクセスで利用できる状態となる。

【００６９】〔４．実施形態の効果〕以上のように、この実施形態では、テーブルＨに格納された利用者の組織

上の属性、すなわち部署や役職に基づいて、各データへのアクセスを認めるかどうか判断される。このため、部門間移動や入社、退職といった異動などで部署や役職が変わる場合、利用者ごとのそれら属性を表す情報のみをメンテナンスすればよく、それに伴って自動的にアクセス権の内容も変わることになる。

【００７０】このため、アクセスするデータごとにパスワードを入力したり、異動のときにパスワードを変えたりデータごとのアクセス権を設定し直すといった煩わしい手数が不要になる。すなわち、個々の利用者について、テーブルH（図１５）に登録されているような部署や役職は、人事部門にある情報のファイルをそのまま流用したり、情報処理部門の作業を要することなく人事部門から直接変更するように構成することが可能である。

【００７１】このため、部署や役職の変動があったとき、アクセス権という観点から改めてアクセス権を設定し直す手数は不要となり、他の人事情報との関係でもアクセス権を矛盾なく容易に管理することができる。つまり、この実施形態によれば、従来のように個々人のアクセス権にかかわる情報を全て変更、作成する場合と比べて、圧倒的に省力化を図ることができる。

【００７２】一方、例えば部署に対する仕事の分担が変更になり文書作成、参照権が変更になったような場合は、参照権テーブルや作成権テーブルといったアクセス権テーブルのみを変更すればよく、利用者の属性にかかわる情報を変更する必要がないので、この点でもアクセス権の管理が非常に容易になる。

【００７３】そして、この実施形態では、テーブルA（図３）に示した文書種類や、テーブルE（図７）に示したようなさらに上位の大分類といった上位概念、すなわち複数の文書を指すくくり単位を使って、性質の共通する複数のデータについてアクセス権をまとめて効率よく設定することができる。

【００７４】特に、この実施形態では、部署と役職の両方に基づいてアクセス権の有無を判断するので、部署ごとに系統化され、階層的な役職制度を持つ多くの組織に適用することが容易である。

【００７５】また、この実施形態では、文書を見るだけの参照、文書の作成、文書の内容の承認といったアクセスの種類に応じて、図１２～１４に示したようにアクセス権を設定できるので、業務の流れや権限の範囲に応じてセキュリティをきめ細かく管理することができる。

【００７６】また、この実施形態では、文書などのデータについて、バージョンごとやページごとといった部分を単位にアクセス権を設定できる。このため、１つのデータでも部分によって性質が違う場合、アクセスを認めるかどうかを無理にデータ全体として決める必要がない。これによって、部分の性質に応じて、アクセスを認めて情報の利用を優先するか、アクセスを認めずにセキュリティを優先するかをきめ細かく設定することが可能となる。

【００７７】また、この実施形態では、組織の内部でも他の部署には秘密にしなければならない機密事項にかかわるデータや、作成途中であるため他の部署に公開する段階にないデータなどについて、テーブルD（図６）に示したように、そのデータを作成した部署など一部の部署の利用者だけにアクセスを限定することができ、セキュリティが一層向上する。

【００７８】また、この実施形態では、ページの内容についても、図９～１１に示したように、リレーショナルデータベース上で扱いやすいテーブル形式で格納するので、実装が容易になる。

【００７９】すなわち、以上のようなこの実施形態では、データに対するアクセス権の設定を、データ種類や大分類といった上位概念でまとめて行うこともできるし、バージョンごとやページごとといったデータの部分を単位として行うこともできる。しかも、それらを単位としたアクセス権の設定を、部署や役職に基づいて行うことができる。

【００８０】このため、適切な種類のデータやデータの適切な部分を、関係のある部署のしかるべき役職者に公開することで、情報の共有とセキュリティを容易に両立することができる。特に、この実施形態では、ログイン時のチェックに加え、文書作成・参照権チェック部４３によってデータに対するアクセス権が確認できたときだけ、データがバージョンやページといったどのような部分を持つかが文書目次表示部４４によって提示される。そしてさらに、ページ作成・参照権チェック部が、アクセスしようとする部分とアクセスの種類についてもアクセス権の確認を行う。このように、利用者に対して段階的に情報を開示することで、システムのセキュリティが一層向上する。

【００８１】なお、この実施形態における文書の具体的な内容としては、例えば基準書、標準書、標準企画書と呼ばれるような技術的内容を記載した文書などを挙げることができ、このような文書では、例えば製品の仕様、規格、取り扱い規定のようにまとまりのある単位ごとに論理ページとして構成し、内容を改訂するごとにバージョンを増やして改訂前のものと改訂後のものを双方保存しておく例などが考えられる。

【００８２】このような例にこの発明を適用することで、例えば、文書のうち各部署に公開するのはもっともバージョンの新しい文書やページとし、それよりバージョンの古い文書やページは担当の役職者だけがアクセスできるようにすることで、不必要な情報の開示を防ぎ、情報の共有を進めながらセキュリティを改善することができる。

【００８３】〔５．他の実施の形態〕なお、この発明は上に述べた実施形態に限定されるものではなく、次に例示するような他の実施の形態も含むものである。例え

ば、上に述べた実施形態では、組織上の属性として部署や役職をコードという形で格納したが、例えば部署か役職のうちどちらか一方だけを使ってもよい。また、例えば正社員と、契約社員、派遣社員のように、部署や役職以外の組織上の属性に基づいてアクセス権があるかどうか判断することもできるし、属性はコードではなく例えば「部長」「課長」といった文字列で格納してもよい。

【００８４】また、上に述べたようないろいろなテーブルは、１つのテーブルあたりの項目数を増やして統合することで総数を減らしてもよく、また、逆に細分化してもよい。また、上に述べた実施形態では、個々の文書を文書種類と大分類という２階層に分ける例を示したが、文書は３階層以上に分けることもできる。

【００８５】また、上に述べた実施形態では、アクセス権の有無を、文書単位とページ単位という２段階に分けて判断したが、判断は１度にまとめて行うこともできる。また、上に述べた実施形態では、データの部分として、データのバージョン、データに含まれるページ、ページのバージョンという３種類を示したが、必ずしもこのような部分に分けてアクセス権を判断する必要はなく、また、これらのうち１種類か２種類だけを導入することもできる。

【００８６】また、機密レベルによって一部の前記部署の利用者にだけアクセスを限定することは必須ではなく、また、ページごとの内容をテーブルに格納することも必須ではない。また、例えば、システムそのものが安全な場所にあり、正規の利用者以外は操作できないような場合は、利用者がデータベースシステムの利用権を持つかどうかをチェックする手段や処理も必須ではない。

【００８７】

【発明の効果】以上のように、この発明によれば、アクセス権を、利用者の組織上の属性と関連づけることで容易に管理変更することができる。

【図面の簡単な説明】

【図１】この発明の実施形態の概略を示す概念図。

【図２】この発明の実施形態の具体的な構成を示す機能ブロック図。

【図３】この発明の実施形態において、文書ＩＤと文書種類などを対照するテーブルＡの内容を例示する図。

【図４】この発明の実施形態において、文書ＩＤとバージョンなどを対照するテーブルＢの内容を例示する図。

【図５】この発明の実施形態において、文書ＩＤと論理ページなどを対照するテーブルＣの内容を例示する図。

【図６】この発明の実施形態において、論理ページと機密レベルなどを対照するテーブルＤの内容を例示する図。

【図７】この発明の実施形態において、文書種類と大分類とを対照するテーブルＥの内容を例示する図。

【図８】この発明の実施形態において、文書種類と論理ページとを対照するテーブルＦの内容を例示する図。

【図９】この発明の実施形態において、論理ページとテーブル名とを対照するテーブルＧの内容を例示する図。

【図１０】この発明の実施形態において、テーブルＴＢＬ０１，ＴＢＬ０２の内容を例示する図。

【図１１】この発明の実施形態において、テーブルＴＢＬ３１，ＴＢＬ３２の内容を例示する図。

【図１２】この発明の実施形態において、文書を単位として参照にかかわるアクセス権を設定する文書参照権テーブルの内容を例示する図。

【図１３】この発明の実施形態において、文書を単位として作成にかかわるアクセス権を設定する文書作成権テーブルの内容を例示する図。

【図１４】この発明の実施形態において、ページを単位として参照にかかわるアクセス権を設定するページ参照権テーブル、及び、ページを単位として作成にかかわるアクセス権を設定するページ作成権テーブルの内容を例示する図。

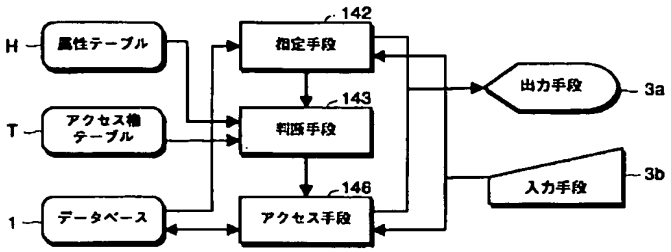
【図１５】この発明の実施形態において、利用者ごとに部署などを対照するテーブルＨの内容を例示する図。

【図１６】この発明の実施形態における処理手順を示すフローチャート。

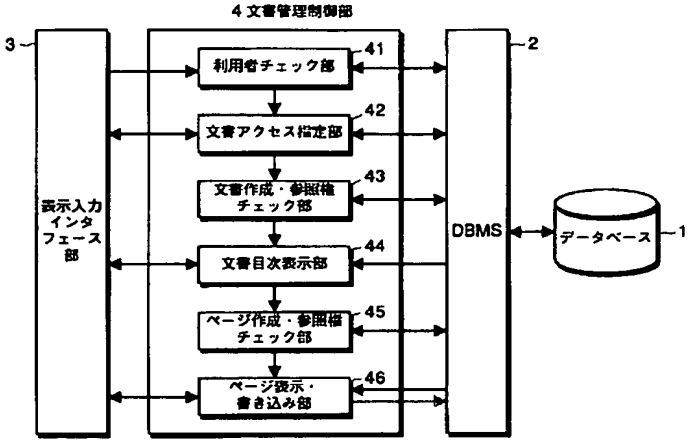
【符号の説明】

１…データベース
２…ＤＢＭＳ
３…表示入力インターフェース部
３ａ…出力手段
３ｂ…入力手段
４…文書管理制御部
４１…利用者チェック部
４２…文書アクセス指定部
１４２…指定手段
４３…文書作成・参照権チェック部
１４３…判断手段
４４…文書目次表示部
４５…ページ作成・参照権チェック部
４６…ページ表示・書き込み部
１４６…アクセス手段
Ｈ…属性テーブル
Ｔ…アクセス権テーブル

【図１】



【図２】



【図５】

【図６】

【図３】

テーブルA

文書ID	文書種別	文書名	所有
A001	TS01	製品B	SA11
A002	MT02	試験法C	ZZK
A003	TS01	製品X	SAPP
A004	TS05	新製品]	X-AF
A005	MT01	製法F	T002
A006	TS05	新製品V	X-BK
A007	MT01	製法G	TS56
A008	MT02	試験法K	ZPJ
:	:	:	:

【図４】

テーブルB

文書ID	文書Ver	発行年月日	備考
A001	1	1995/2/5	
A001	2	1997/3/1	
A002	1	1995/5/8	
A003	1	1995/9/12	
A003	2	1996/1/20	
A003	3	1997/5/30	
:	:	:	

テーブルC

文書ID	文書Ver	論理ページ	ページVer
A001	1	PS01	1
A001	1	PS02	1
A001	1	PS03	1
A001	2	PS01	1
A001	2	PS02	2
A001	2	PS03	1
A002	1	PF01	1
A002	1	PF02	1
:	:	:	:

テーブルD

文書ID	論理ページ	ページVer	機密レベル	作成部署
A001	PS01	1		BUA01
A001	PS02	1		BUA01
A001	PS03	1	BUA02	BUA01
A001	PS02	2		BUA01
A002	PF01	1		BUM02
A002	PF02	1		BUM02
:	:	:	:	:

【図１１】

テーブルG

論理ページ	テーブル名
PS01	TBL01
PS01	TBL02
PS02	TBL11
:	:
PF01	TBL31
PF01	TBL32
:	:

【図１２】

TBL31

文書ID	ページVer	使用装置	試験法説明	備考
A002	1	TYPE-A	注意すべき･･	
A008	1	TYPE-S	サブAは･･	
A008	2	TYPE-S	改良した･･	
:	:	:	:	:

TBL32

文書ID	ページVer	ファイル名
A002	1	DATA-010
A002	1	DATA-011
A008	1	DATA-020
A008	2	DATA-021
:	:	:

【図９】

TBL01

文書ID	ページVer	成分名	量	単位
A001	1	精製剤	5	%
A001	1	溶媒	8	%
A001	1	活性剤	10	%
A001	1	香料	1	%
A001	2	精製剤	5	%
A001	2	溶媒	9	%
A001	2	活性剤	12	%
A001	2	香料	1	%
:	:	:	:	:

TBL02

文書ID	ページVer	説明
A001	1	洗剤成分の･･
A001	2	新しい製品は･･
A003	1	植物の成分･･
:	:	:

【図１３】

文書参照権テーブル

大分類	文書種別	閲覧	改編
TS-A	TS01	BUA*	*
TS-A	TS02	*	A
TS-A	TS02	*	B
TS-A	TS03	BUG01	*
TS-A	TS03	BUG02	A
TS-A	TS03	BUG03	*
TS-B	*	*	*
:	:	:	:

【図７】

テーブルE

大分類	文書種別
TS-A	TS01
TS-A	TS02
TS-A	TS03
TS-B	TS04
TS-B	TS05
:	:
MT-A	MT01
MT-B	MT02
:	:

【図８】

テーブルF

文書種別	論理ページ
TS01	PS01
TS01	PS02
TS01	PS03
TS02	PT01
TS02	PT02
TS03	PU01
TS03	PU02
TS03	PU03
:	:
MT01	PM01
MT02	PF01
MT02	PF02
:	:

【図１０】

【図１４】

ページ参照権テーブル

論理ページ	部署	役職
PS01	*	B
PS01	*	A
PS02	*	*
PS03	BUA01	*
:	:	:

ページ作成権テーブル

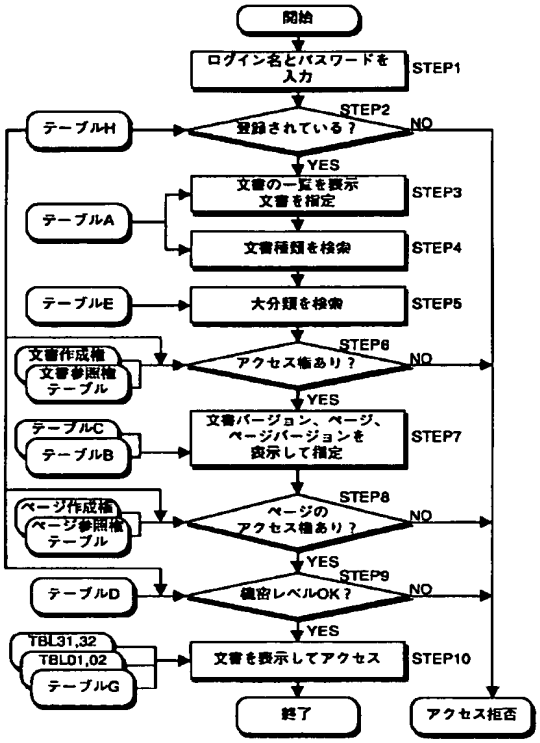
論理ページ	部署	役職
PS01	BUA01	A
PS01	BUA01	B
PS02	BUA01	B
PS03	BUA01	*
:	:	:

【図１５】

テーブルH

ログイン名	パスワード	社員名	部署コード	役職コード
S9501234	JSD3R	佐藤太郎	BUA01	A
S9502366	TY2PRT	鈴木一郎	BUA02	B
S9615235	S5RRTY	小林花子	BUC01	A
S9825482	9501522	山本正夫	BUA01	C
:	:	:	:	:

【図１６】



フロントページの続き

(72)発明者　江畑　利一
東京都墨田区本所１丁目３番７号　ライオン株式会社内
(72)発明者　西條　一彦
東京都墨田区本所１丁目３番７号　ライオン株式会社内
(72)発明者　小林　明人
東京都新宿区西新宿２丁目６番１号　株式会社シーエスケイ内

Ｆターム(参考)　5B017 AA07 BA05 BA06 BB06 CA16
5B082 BA09 EA11 GA05 GA13 GC03
GC04
5B085 AE06

【図５】

機密ランク		個秘	マル秘	社外秘	一般	管理者権限
所属	申請者	原本	原本	原本	原本	なし
	審査者	原本	原本	原本	原本	なし
	承認者	原本	原本	原本	原本	なし
利用者	役員	原本	原本	原本	原本	なし
	社員	×	書庫＋承約△	書庫＋承約△	印刷可能閲覧文書	あり
	関連企業社員	×	▲＋記名文書	▲＋記名文書	▲	なし
	派遣契約社員	×	×	×	▲	一部あり

△閲覧申請により原本閲覧可能
▲閲覧申請により印刷不可能閲覧可能
×不可

フロントページの続き

Ｆターム(参考)　5B009 SA12
5B075 KK07 KK43 KK54 KK63 KK66
ND03 NS10 UU06
5B082 EA11 EA12 GA13